Administratorhandbuch

AWS Wickr

AWS Wickr: Administratorhandbuch

Table of Contents

Was ist AWS Wickr?

AWSWickr ist ein end-to-end verschlüsselter Dienst, der Organisationen und Regierungsbehörden bei der sicheren Kommunikation über one-to-one und Gruppennachrichten, Sprach- und Videoanrufe, Dateifreigabe, Bildschirmübertragung und mehr hilft. Wickr kann Kunden dabei helfen, Datenaufbewahrungspflichten im Zusammenhang mit Messaging-Apps für Privatanwender zu erfüllen und die Zusammenarbeit auf sichere Weise zu erleichtern. Fortschrittliche Sicherheits- und Verwaltungskontrollen helfen Unternehmen dabei, gesetzliche und behördliche Anforderungen zu erfüllen und maßgeschneiderte Lösungen für Herausforderungen im Bereich der Datensicherheit zu entwickeln.

Informationen können zu Aufbewahrungs- und Prüfzwecken in einem privaten, vom Kunden kontrollierten Datenspeicher protokolliert werden. Benutzer haben umfassende administrative Kontrolle über Daten. Dazu gehören das Festlegen von Berechtigungen, das Konfigurieren kurzlebiger Nachrichtenoptionen und das Definieren von Sicherheitsgruppen. Wickr lässt sich in zusätzliche Dienste wie Active Directory (AD), Single Sign-On (SSO) mit OpenID Connect (OIDC) und mehr integrieren. Über die können Sie schnell ein Wickr-Netzwerk erstellen und verwalten und Workflows mithilfe von Wickr-Bots sicher automatisieren. AWS Management Console Um zu beginnen, sehen Sie sich Einrichtung für AWS Wickr an.

Themen

Funktionen von Wickr

Verbesserte Sicherheit und Datenschutz

Wickr verwendet für jede Funktion die 256-Bit-Verschlüsselung Advanced end-to-end Encryption Standard (AES). Die Kommunikation wird lokal auf den Benutzergeräten verschlüsselt und bleibt bei der Übertragung an andere Personen als Absender und Empfänger nicht entzifferbar. Jede Nachricht, jeder Anruf und jede Datei wird mit einem neuen zufälligen Schlüssel verschlüsselt, und niemand außer den vorgesehenen Empfängern (auch nicht AWS) kann sie entschlüsseln. Ganz gleich,

ob sie sensible und regulierte Daten teilen, Rechts- oder Personalfragen besprechen oder sogar taktische militärische Operationen durchführen — Kunden nutzen Wickr, um zu kommunizieren, wenn Sicherheit und Datenschutz an erster Stelle stehen.

Datenaufbewahrung

Flexible Verwaltungsfunktionen dienen nicht nur dem Schutz sensibler Informationen, sondern auch der Aufbewahrung von Daten, soweit dies für Compliance-Verpflichtungen, gesetzliche Aufbewahrungsfristen und Prüfungszwecke erforderlich ist. Nachrichten und Dateien können in einem sicheren, vom Kunden kontrollierten Datenspeicher archiviert werden.

Flexibler Zugriff

Benutzer haben Zugriff auf mehrere Geräte (Mobil, Desktop) und können in Umgebungen mit geringer Bandbreite arbeiten, einschließlich Verbindungsabbrüchen und Kommunikationsverbindungen. out-of-band

Administrative Kontrollen

Benutzer haben umfassende administrative Kontrolle über Daten. Dazu gehören das Festlegen von Berechtigungen, das Konfigurieren von Optionen für verantwortungsbewusstes kurzlebiges Messaging und das Definieren von Sicherheitsgruppen.

Leistungsstarke Integrationen und Bots

Wickr lässt sich in zusätzliche Dienste wie Active Directory, Single Sign-On (SSO) mit OpenID Connect (OIDC) und mehr integrieren. Kunden können damit schnell ein Wickr-Netzwerk erstellen und verwalten und Workflows mit Wickr Bots sicher automatisieren. AWS Management Console

Im Folgenden finden Sie eine Aufschlüsselung der Kooperationsangebote von Wickr:

- Einzel- und Gruppennachrichten: Chatten Sie sicher mit Ihrem Team in Räumen mit bis zu 500 Mitgliedern
- Audio- und Videoanrufe: Halten Sie Telefonkonferenzen mit bis zu 70 Personen ab
- Bildschirmübertragung und Übertragung: Präsentieren Sie mit bis zu 500 Teilnehmern
- Dateien teilen und speichern: Übertragen Sie bis zu 5 Dateien GBs mit unbegrenztem Speicherplatz
- Kurzlebig: Kontrolliere den Ablauf und die Timer burn-on-read
- Globaler Verband: Connect zu Wickr-Benutzern außerhalb Ihres Netzwerks her

> **Note**
>
> Wickr-Netzwerke in AWS GovCloud (US-West) können nur mit anderen Wickr-Netzwerken in (US-West) verbunden werden. AWS GovCloud

Auf Wickr zugreifen

Wickr ist in den USA Ost (Nord-Virginia), Kanada (Zentral), Europa (London), Asien-Pazifik (Sydney), Europa (Frankfurt), Europa (Stockholm), Europa (Zürich), Asien-Pazifik (Singapur) und Asien-Pazifik (Tokio) verfügbar. AWS-Regionen Wickr ist auch WickrGov in den AWS GovCloud (USA West) erhältlich. AWS-Region

Administratoren greifen auf das AWS Management Console für Wickr unter zu. https://console.aws.amazon.com/wickr/ Bevor Sie mit der Verwendung von Wickr beginnen, sollten Sie die Anleitungen Einrichtung für AWS Wickr undErste Schritte mit AWS Wickr.

> **Note**
>
> Der Wickr-Dienst hat keine Anwendungsprogrammierschnittstelle ()API.

Endbenutzer greifen über den Wickr-Client auf Wickr zu. Weitere Informationen finden Sie im AWSWickr-Benutzerhandbuch.

Preisgestaltung

Wickr ist in verschiedenen Tarifen für Einzelpersonen, kleine Teams und große Unternehmen erhältlich. Weitere Informationen finden Sie unter AWSWickr Pricing.

Wickr-Dokumentation für Endbenutzer

Wenn Sie ein Endbenutzer des Wickr-Clients sind und auf dessen Dokumentation zugreifen müssen, lesen Sie das AWSWickr-Benutzerhandbuch.

Einrichtung für AWS Wickr

Wenn du neu bist AWS Kunde, erfüllen Sie die auf dieser Seite aufgeführten Einrichtungsvoraussetzungen, bevor Sie AWS Wickr verwenden. Für diese Einrichtungsverfahren verwenden Sie AWS Identity and Access Management (IAM) Dienst. Vollständige Informationen zu IAM finden Sie im IAMBenutzerhandbuch.

Themen

Melden Sie sich an für AWS

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um einen zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/die Anmeldung.
2. Folgen Sie den Online-Anweisungen.

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, ein Root-Benutzer des AWS-Kontoswird erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen im Konto. Als bewährte Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

Erstellen eines IAM-Benutzers

Wählen Sie zum Erstellen eines Administratorbenutzers eine der folgenden Optionen aus.

Wählen Sie eine Möglichkeit zur Verwaltung Ihres Administrators aus.	Bis	Von	Sie können auch
Im IAM Identity Center (Empfohlen)	Verwenden Sie kurzfristige Zugangsdaten für den Zugriff AWS. Dies steht im Einklang mit den bewährten Methoden für die Sicherheit. Informationen zu bewährten Methoden finden Sie unter Bewährte Sicherheitsmethoden IAM im IAM Benutzerhandbuch.	Folgen Sie den Anweisungen unter Erste Schritte im AWS IAM Identity Center Benutzerleitfaden.	Konfigurieren Sie den programmatischen Zugriff, indem Sie AWS CLI zu verwenden AWS IAM Identity Center in der AWS Command Line Interface Benutzerleitfaden.
In IAM (Nicht empfohlen)	Verwenden Sie langfristige Anmeldeinformationen für den Zugriff AWS.	Folgen Sie den Anweisungen unter Erstellen Ihres ersten IAM Admin-Benutzers und Ihrer ersten Administrator-Benutzergruppe im IAMBenutzerhandbuch.	Konfigurieren Sie den programmatischen Zugriff, indem Sie im Benutzerhandbuch die Zugriffsschlüssel für IAM IAM Benutzer verwalten.

> **Note**
>
> Sie können die `AWSWickrFullAccess` verwaltete Richtlinie auch zuweisen, um dem Wickr-Dienst volle Administratorrechte zu gewähren. Weitere Informationen finden Sie unter AWS verwaltete Richtlinie: AWSWickrFullAccess.

Was kommt als Nächstes

Sie haben die erforderlichen Schritte zur Einrichtung abgeschlossen. Informationen zum Konfigurieren von Wickr finden Sie unterErste Schritte.

Erste Schritte mit AWS Wickr

In diesem Handbuch zeigen wir Ihnen, wie Sie mit Wickr beginnen können, indem Sie ein Netzwerk erstellen, Ihr Netzwerk konfigurieren und Benutzer erstellen.

Themen

Voraussetzungen

Bevor Sie beginnen, stellen Sie sicher, dass Sie die folgenden Voraussetzungen erfüllen, falls Sie dies noch nicht getan haben:

- Melden Sie sich für Amazon Web Services an (AWS). Weitere Informationen finden Sie unter Einrichtung für AWS Wickr.
- Stellen Sie sicher, dass Sie über die erforderlichen Berechtigungen verfügen, um Wickr zu verwalten. Weitere Informationen finden Sie unter AWS verwaltete Richtlinie: AWSWickrFullAccess.
- Stellen Sie sicher, dass Sie die entsprechenden Ports und Domänen für Wickr zulassen. Weitere Informationen finden Sie unter Liste der Ports und Domänen, die zugelassen werden sollen.

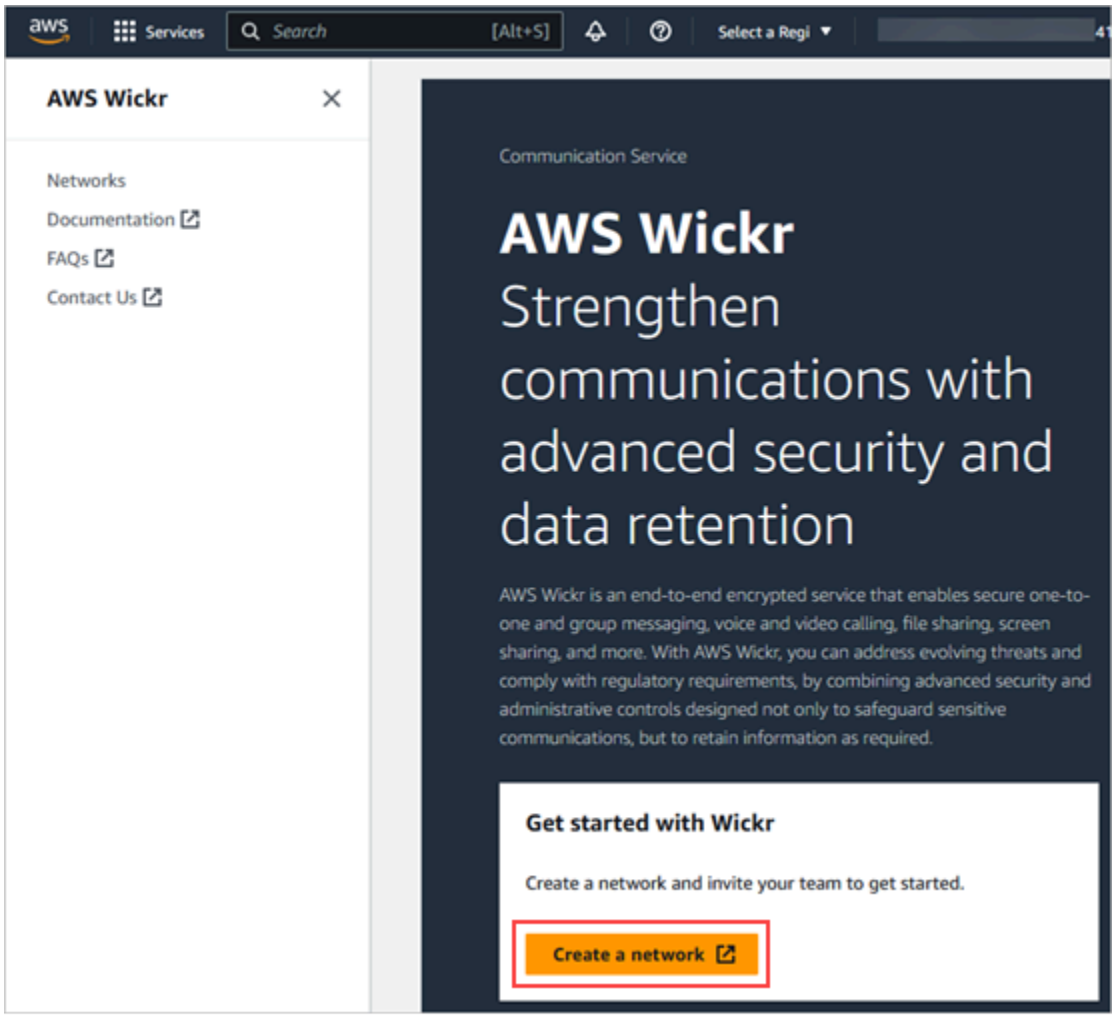
Schritt 1: Erstellen Sie ein Netzwerk

Gehen Sie wie folgt vor, um ein Wickr-Netzwerk für Ihr Konto zu erstellen.

1. Öffnen Sie das AWS Management Console für Wickr unter. https://console.aws.amazon.com/wickr/

> **Note**
>
> Wenn Sie noch kein Wickr-Netzwerk erstellt haben, wird die Informationsseite für den Wickr-Dienst angezeigt. Nachdem Sie ein oder mehrere Wickr-Netzwerke erstellt haben, wird die Netzwerkseite angezeigt, die eine Listenansicht aller von Ihnen erstellten Wickr-Netzwerke enthält.

2. Wählen Sie Create a network (Netzwerk erstellen).



3. Geben Sie im Textfeld Netzwerkname einen Namen für Ihr Netzwerk ein. Wählen Sie einen Namen, den die Mitglieder Ihrer Organisation wiedererkennen, z. B. den Namen Ihres Unternehmens oder den Namen Ihres Teams.
4. Wählen Sie einen Plan. Sie können einen der folgenden Wickr-Netzwerkpläne wählen:

- Standard — Für kleine und große Unternehmensteams, die administrative Kontrollen und Flexibilität benötigen.
- Premium - oder kostenlose Premium-Testversion — Für Unternehmen, die höchste Funktionseinschränkungen, detaillierte Verwaltungskontrollen und Datenspeicherung benötigen.

Administratoren können die kostenlose Premium-Testoption wählen, die für bis zu 30 Benutzer verfügbar ist und drei Monate gültig ist. Dieses Angebot gilt für neue, legacy-freie Testversionen und Standardpläne. Administratoren können während der kostenlosen Premium-Testphase ein Upgrade oder Downgrade auf Premium- oder Standard-Tarife durchführen.

Weitere Informationen zu den verfügbaren Wickr-Plänen und Preisen finden Sie auf der Wickr-Preisseite.

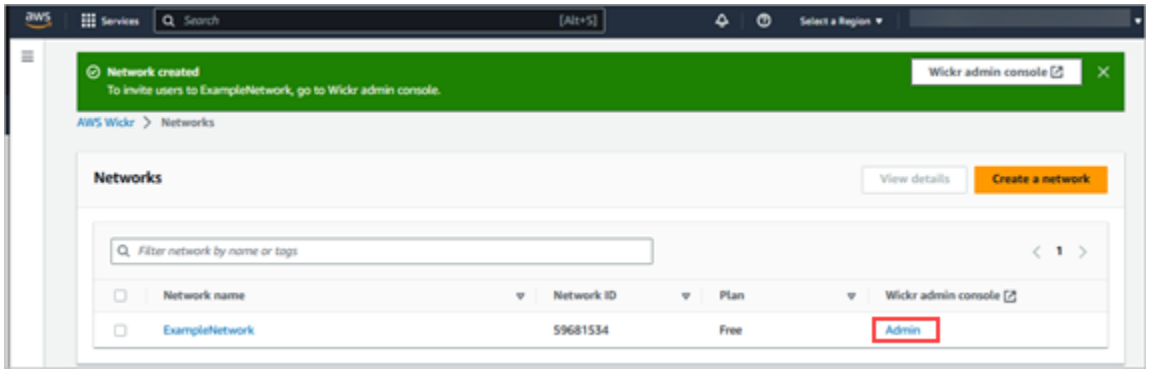
5. (Optional) Wählen Sie Neues Tag hinzufügen, um Ihrem Netzwerk ein Tag hinzuzufügen. Tags bestehen aus einem Schlüssel-Wert-Paar. Tags können verwendet werden, um Ressourcen zu suchen und zu filtern oder Ihre AWS Kosten zu verfolgen. Weitere Informationen finden Sie unter Netzwerk-Tags.
6. Wählen Sie „Netzwerk erstellen“.

   Sie werden auf die Netzwerkseite von AWS Management Console for Wickr weitergeleitet, und das neue Netzwerk wird auf der Seite aufgeführt.

Schritt 2: Konfigurieren Sie Ihr Netzwerk

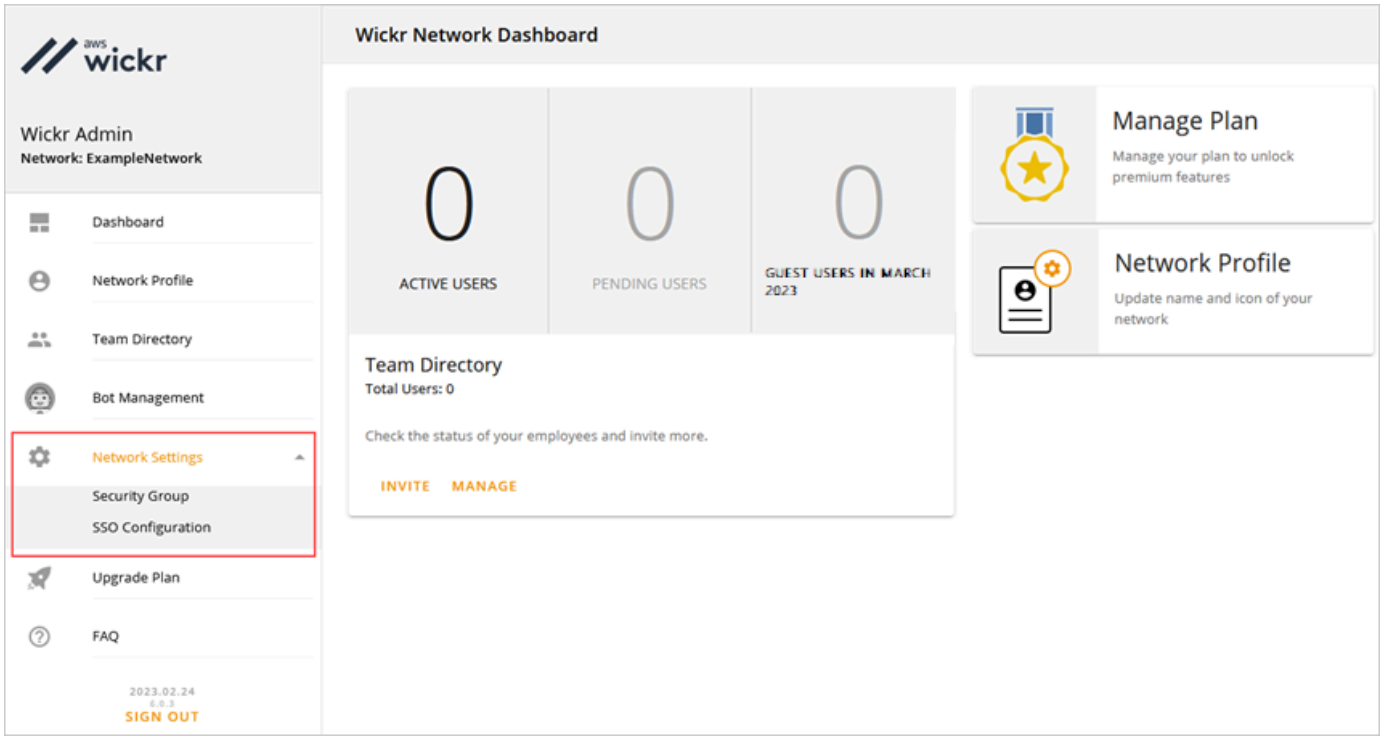
Gehen Sie wie folgt vor, um auf die Wickr Admin Console zuzugreifen, in der Sie Benutzer hinzufügen, Sicherheitsgruppen hinzufügen, die Datenspeicherung konfigurieren und weitere Netzwerkeinstellungen konfigurieren können. SSO

1. Wählen Sie auf der Seite Netzwerke den Link Admin, um zur Wickr Admin Console für dieses Netzwerk zu gelangen.



Sie werden zur Wickr Admin Console für das ausgewählte Netzwerk weitergeleitet.

2. Wählen Sie im Navigationsbereich der Wickr Admin Console Netzwerkeinstellungen.



Die folgenden Netzwerkeinstellungsoptionen sind verfügbar. Weitere Informationen zur Konfiguration dieser Einstellungen finden Sie unterVerwalte dein AWS Wickr-Netzwerk.

- Sicherheitsgruppe — Verwalten Sie Sicherheitsgruppen und ihre Einstellungen, z. B. Richtlinien zur Kennwortkomplexität, Nachrichteneinstellungen, Anruffunktionen, Sicherheitsfunktionen und externen Verbund. Weitere Informationen finden Sie unter Sicherheitsgruppen.
- SSOKonfiguration — Konfigurieren Sie die Endpunktadresse für Ihr Wickr-Netzwerk SSO und zeigen Sie sie an. Wickr unterstützt nur SSO Anbieter, die OpenID Connect (OIDC)

verwenden. Anbieter, die Security Assertion Markup Language (SAML) verwenden, werden nicht unterstützt. Weitere Informationen finden Sie unter Konfiguration von Single Sign-On.

Schritt 3: Benutzer erstellen und einladen

Sie können Benutzer in Ihrem Wickr-Netzwerk mit den folgenden Methoden erstellen:

- Single Sign-On — Wenn Sie es konfigurierenSSO, können Sie Benutzer einladen, indem Sie Ihre Wickr-Unternehmens-ID teilen. Endbenutzer registrieren sich mit der angegebenen Firmen-ID und ihrer geschäftlichen E-Mail-Adresse für Wickr. Weitere Informationen finden Sie unter Konfiguration von Single Sign-On.
- Einladung — Sie können Benutzer in The AWS Management Console for Wickr manuell erstellen und sich eine E-Mail-Einladung zusenden lassen. Endbenutzer können sich für Wickr registrieren, indem sie den Link in der E-Mail auswählen.

> **Note**
>
> Sie können auch Gastbenutzer für Ihr Wickr-Netzwerk aktivieren. Die Gastbenutzerfunktion befindet sich derzeit in der Vorschauversion. Weitere Informationen finden Sie unter Gastnutzer

Gehen Sie wie folgt vor, um Benutzer zu erstellen oder einzuladen.

> **Note**
>
> Administratoren gelten ebenfalls als Benutzer und müssen sich selbst zu Netzwerken einladen, die nicht zu SSO SSO Wickr-Netzwerken gehören.

SSO

Schreiben und senden Sie eine E-Mail an die SSO Benutzer, die sich für Wickr registrieren sollen. Nehmen Sie die folgenden Informationen in Ihre E-Mail auf:

- Ihre Wickr-Firmen-ID. Sie geben bei der Konfiguration eine Unternehmens-ID für Ihr Wickr-Netzwerk an. SSO Weitere Informationen finden Sie unter Konfigurieren SSO.

- Die E-Mail-Adresse, die sie für die Anmeldung verwenden sollten.
- DannURL, um den Wickr-Client herunterzuladen. Benutzer können die Wickr-Clients von der AWS Wickr-Downloadseite unter download/ herunterladen. https://aws.amazon.com/wickr/

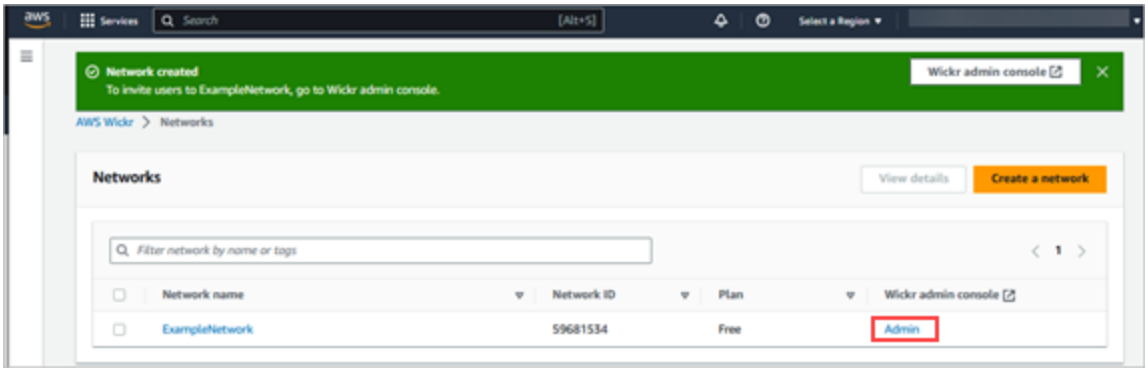
> **Note**
>
> Wenn Sie Ihr Wickr-Netzwerk in AWS GovCloud (US-West) erstellt haben, weisen Sie Ihre Benutzer an, den Client herunterzuladen und zu installieren. WickrGov Weisen Sie Ihre Benutzer für alle anderen AWS Regionen an, den Standard-Wickr-Client herunterzuladen und zu installieren. Weitere Informationen zu AWS WickrGov finden Sie AWS WickrGovim AWS GovCloud (US) Benutzerhandbuch.

Wenn sich Benutzer für Ihr Wickr-Netzwerk registrieren, werden sie dem Wickr-Teamverzeichnis mit dem Status Aktiv hinzugefügt.

Non-SSO

Um Wickr-Benutzer manuell zu erstellen und Einladungen zu versenden:

1. Öffnen Sie sie AWS Management Console für Wickr unter. https://console.aws.amazon.com/wickr/
2. Wählen Sie auf der Seite Netzwerke den Link Admin, um zur Wickr Admin Console für dieses Netzwerk zu navigieren.



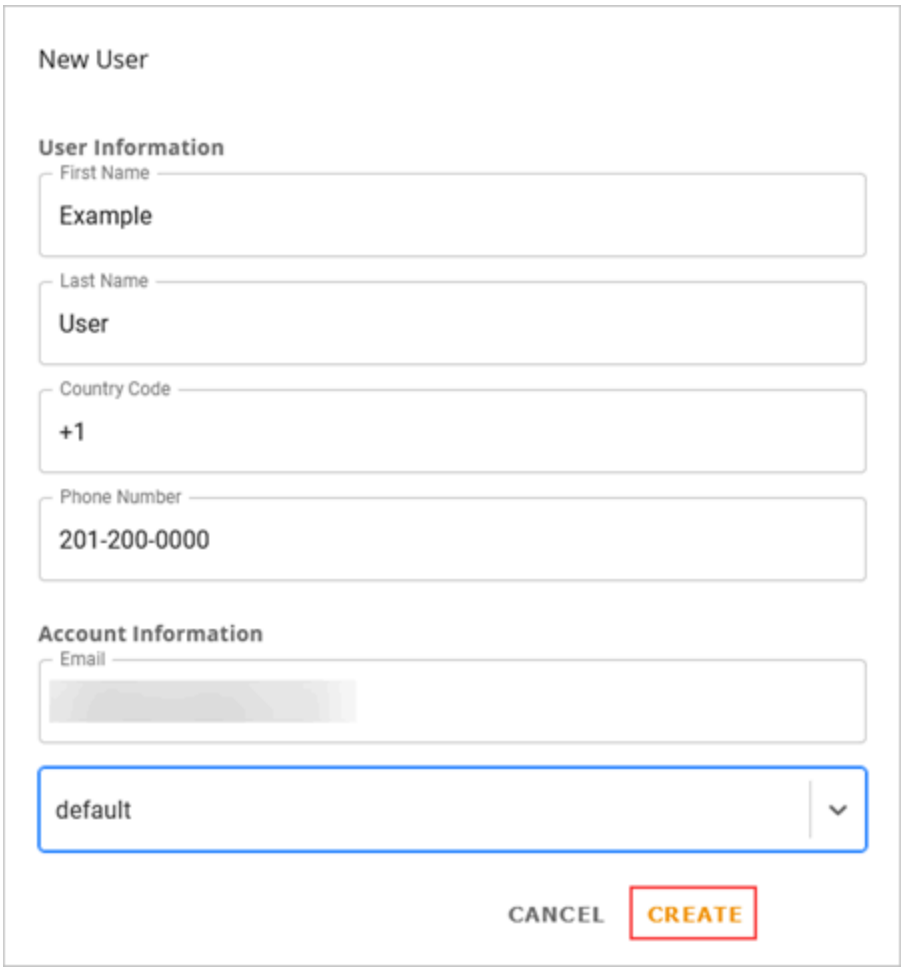
Sie werden zur Wickr Admin Console für ein bestimmtes Netzwerk weitergeleitet. In der Wickr Admin Console können Sie Benutzer hinzufügen, Sicherheitsgruppen hinzufügen, die Datenspeicherung konfigurieren und weitere Einstellungen für das von Ihnen ausgewählte Netzwerk vornehmen. SSO

3. Wählen Sie im Navigationsbereich der Wickr Admin Console Benutzer und dann Teamverzeichnis aus.

   Auf der Seite Benutzer können Sie einzelne Benutzer hinzufügen, indem Sie Neuen Benutzer erstellen wählen. Sie können auch mehrere Benutzer gleichzeitig hinzufügen, indem Sie im oberen Navigationsbereich auf das Symbol Benutzer hinzufügen klicken. Wählen Sie das CSVDownload-Symbol, um eine CSV Vorlage herunterzuladen, die Sie bearbeiten und zusammen mit Ihrer Benutzerliste hochladen können.

4. Geben Sie den Vornamen, Nachnamen, die Landesvorwahl, die Telefonnummer und die E-Mail-Adresse des Benutzers ein. Die E-Mail-Adresse ist das einzige Feld, das erforderlich ist. Achten Sie darauf, die passende Sicherheitsgruppe für den Benutzer auszuwählen.

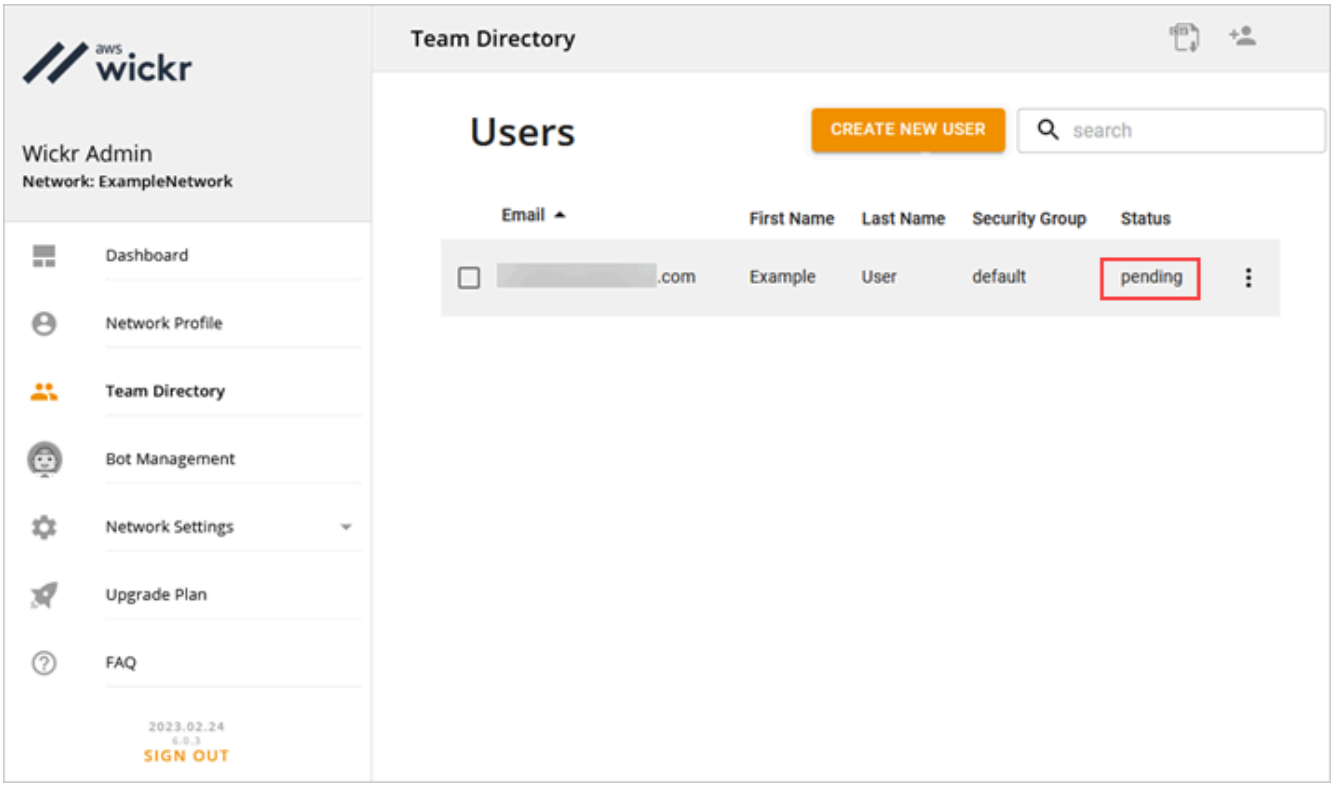
5. Wählen Sie Create (Erstellen) aus.



   Wickr sendet eine Einladungs-E-Mail an die Adresse, die Sie für den Benutzer angegeben haben. Die E-Mail enthält Download-Links für die Wickr-Client-Anwendungen und einen Link zur Registrierung für Wickr. Weitere Informationen darüber, wie diese Endbenutzererfahrung

aussieht, finden Sie im Wickr-Benutzerhandbuch unter Wickr-App herunterladen und Ihre Einladung annehmen. AWS

Wenn sich Benutzer über den Link in der E-Mail für Wickr registrieren, ändert sich ihr Status im Wickr-Teamverzeichnis von Ausstehend auf Aktiv.



Nächste Schritte

Sie haben die Schritte „Erste Schritte“ abgeschlossen. Informationen zur Verwaltung von Wickr finden Sie in den folgenden Anleitungen:

- Verwalte dein AWS Wickr-Netzwerk
- Benutzer in AWS Wickr verwalten

Übertragen Sie Wickr Pro auf Wickr AWS

> **Note**
>
> Wickr Pro wurde eingestellt. Wenn Sie den Zugriff auf Wickr Pro verloren haben, folgen Sie den Schritten in dieser Anleitung, um zu Wickr zu AWS wechseln.

In diesem Handbuch zeigen wir Ihnen, wie Sie von Wickr Pro wechseln und Wickr verwenden können. AWS

Folgen Sie den Schritten in dieser Anleitung, wenn Sie bereits ein Wickr Pro-Netzwerk haben, aber noch eines NOT haben. AWS-Konto Bitte wenden Sie sich bei jedem Schritt an den Support, wenn Sie Hilfe benötigen.

Wenn Ihre Organisation bereits über ein AWS Konto verfügt, füllen Sie das Formular „Von Wickr Pro zu AWS Wickr migrieren“ aus. Der AWS Wickr-Support hilft Ihnen dann weiter.

Sie benötigen eine AWS-Konto ID, um Ihr AWS Wickr-Netzwerk als Benutzer verwalten zu können. AWS-Service Weitere Informationen darüber, was ein AWS-Konto ist und wie das Konto verwaltet wird, finden Sie im Referenzhandbuch zur AWS Kontoverwaltung.

Themen

Schritt 1: Erstellen Sie ein AWS Konto

Gehen Sie wie folgt vor, um ein AWS Konto zu erstellen.

1. Wenn Ihre Organisation noch keine AWS Konto-ID hat, können Sie damit beginnen, eine eigenständige AWS Konto-ID zu erstellen. Ein paar wichtige Dinge, die Sie dafür benötigen:
   - Eine Kredit-/Debitkarte für die Abrechnung
   - Eine E-Mail-Adresse, auf die eine Gruppe zugreifen kann (empfohlen, nicht erforderlich)

- Wählen Sie einen AWS Support Plan aus. Weitere Informationen finden Sie unter AWS Support Pläne ändern.

> **Note**
>
> Sie können Ihren AWS Support Plan jederzeit ändern, wenn Sie mehr über Ihre Bedürfnisse erfahren.

2. IAMAls bewährte Sicherheitsmethode sollten Sie Administratorzugriff einrichten (optional, aber empfohlen). Weitere Informationen finden Sie unter AWS Identity and Access Management. Genauere Anweisungen zum administrativen Zugriff auf AWS Wickr finden Sie unter AWS Verwaltete Richtlinie: AWSWickrFullAccess.
3. Sobald Sie die vorherigen Schritte abgeschlossen haben, können Sie sich bei der anmelden, um Ihre 12-stellige AWS-Konto ID unter Ihrem Kontonamen AWS Management Console zu finden.

Schritt 2: Rufen Sie Ihre Wickr-Netzwerk-ID ab

Gehen Sie wie folgt vor, um Ihre Wickr-Netzwerk-ID abzurufen.

1. Melden Sie sich bei Ihrer aktuellen Wickr-Administrationskonsole an und wählen Sie die Netzwerke aus, die Sie migrieren möchten, und wählen Sie dann Netzwerkprofil aus.
2. Auf der Netzwerkprofilseite wird Ihre Netzwerk-ID angezeigt. Dabei handelt es sich um eine 8-stellige numerische ID.

Schritt 3: Senden Sie eine Anfrage

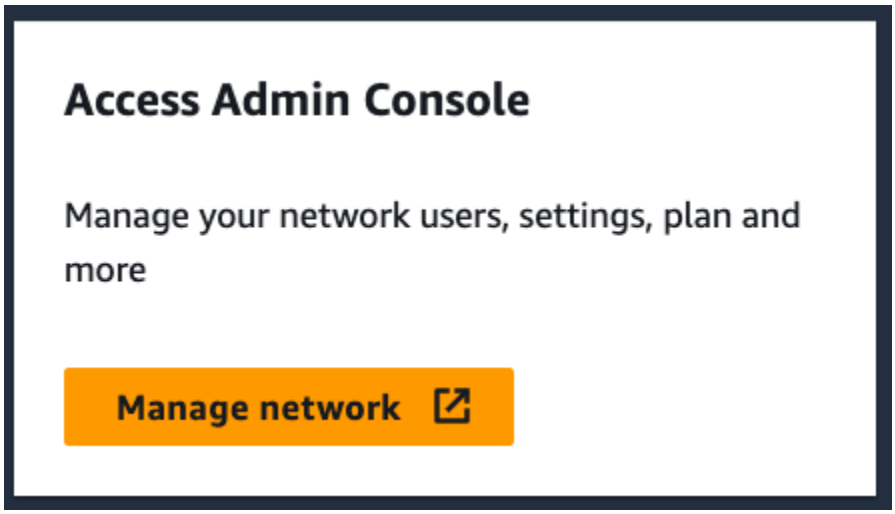
Nachdem Sie Ihre AWS-Konto ID und die Wickr Pro-Netzwerk-ID haben, müssen Sie das Formular „Von Wickr Pro zu AWS Wickr migrieren“ ausfüllen.

Nach dem Ausfüllen, in der Regel innerhalb von 14 Tagen, wird sich ein Mitarbeiter des AWS Wickr-Supports mit Ihnen in Verbindung setzen, um zu bestätigen, dass Ihr Wickr-Netzwerk zu Ihrem hinzugefügt wurde. AWS-Konto

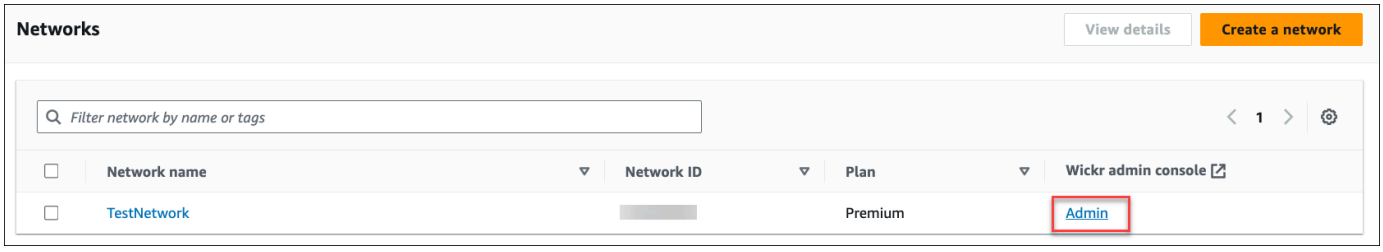
Schritt 4: Loggen Sie sich in Ihre Konsole ein AWS

> **Note**
>
> Folgen AFTER Sie diesen Schritten, um eine Bestätigung zu erhalten, dass Ihr Wickr Pro-Netzwerk zu Ihrem AWS-Konto hinzugefügt wurde.

1. Sie können sich bei der AWS Konsole als Root-Benutzer ODER mit einem IAM Benutzer anmelden, den Sie zuvor (wie empfohlen) in Schritt 2 für AWS Wickr erstellt haben.
2. Navigieren Sie zu Ihrem AWS Wickr-Dienst. Sie können dies über das Menü Dienste tun oder indem Sie in der Suchleiste nach AWS Wickr suchen.
3. Wählen Sie auf der AWS Wickr-Seite Netzwerk verwalten aus, um auf Ihre Wickr-Netzwerkliste zuzugreifen.



4. Wählen Sie auf der Seite Netzwerke in der Spalte Wickr-Administrationskonsole den Link Admin rechts neben dem gewünschten Netzwerknamen aus.



5. Die Übertragung ist jetzt abgeschlossen! Sie werden Ihr Wickr-Netzwerk-Dashboard sehen.

Die Abrechnung für Ihr Netzwerk wird nun auf Ihr AWS-Kontoübertragen. Es kann bis zu 3 Werktage dauern, bis sich der Support mit einer Bestätigung bei Ihnen meldet. Nachdem Sie Ihre Bestätigung erhalten haben, können Sie Ihre Rechnung über die AWS Konsole einsehen und bezahlen.

Verwalte dein AWS Wickr-Netzwerk

Im Bereich Netzwerkeinstellungen der AWS Management Console für Wickr können Sie Ihren Wickr-Netzwerknamen, Ihre Sicherheitsgruppen, Ihre SSO Konfiguration und Ihre Datenaufbewahrungseinstellungen verwalten.

Themen

Netzwerkprofil

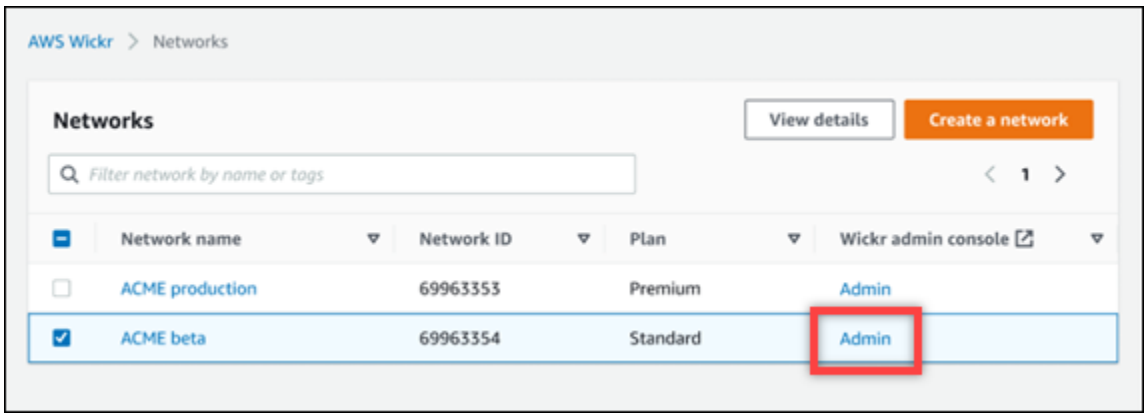
Sie können den Namen Ihres Wickr-Netzwerks bearbeiten und Ihre Netzwerk-ID im Bereich Netzwerkprofil der AWS Management Console für Wickr.

Themen

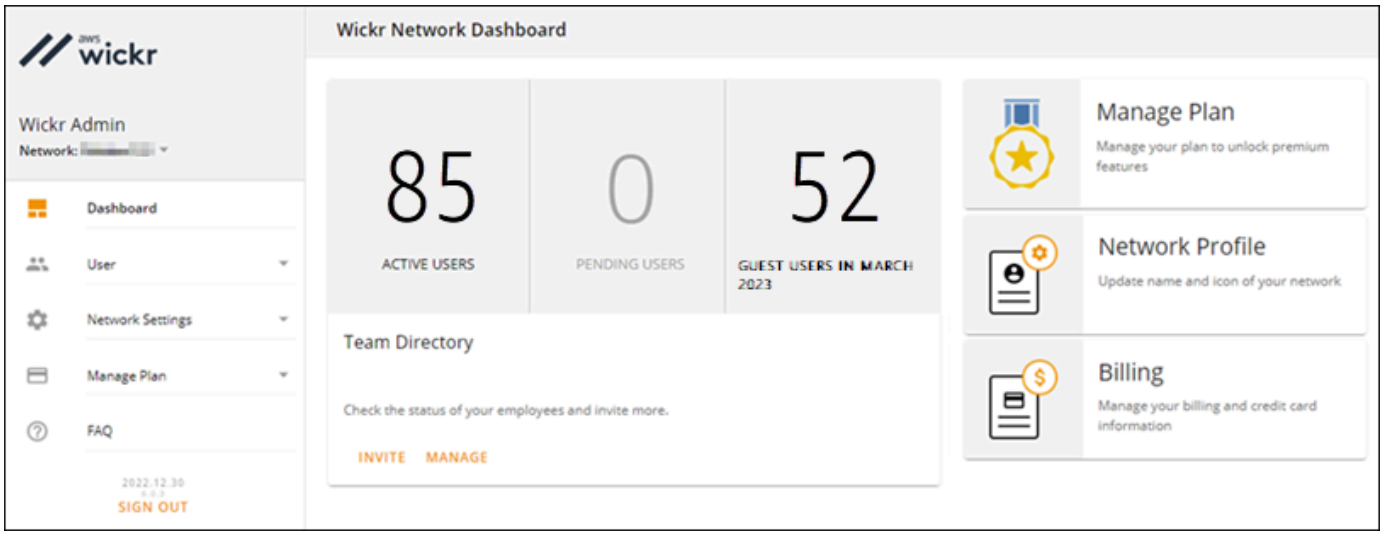
Netzwerkprofil anzeigen

Gehen Sie wie folgt vor, um Ihr Wickr-Netzwerkprofil und Ihre Netzwerk-ID anzuzeigen.

1. Öffnen Sie AWS Management Console für Wickr bei. https://console.aws.amazon.com/wickr/
2. Wählen Sie auf der Seite Netzwerke den Link Admin, um zur Wickr Admin Console für dieses Netzwerk zu gelangen.



Sie werden zur Wickr Admin Console für ein bestimmtes Netzwerk weitergeleitet.



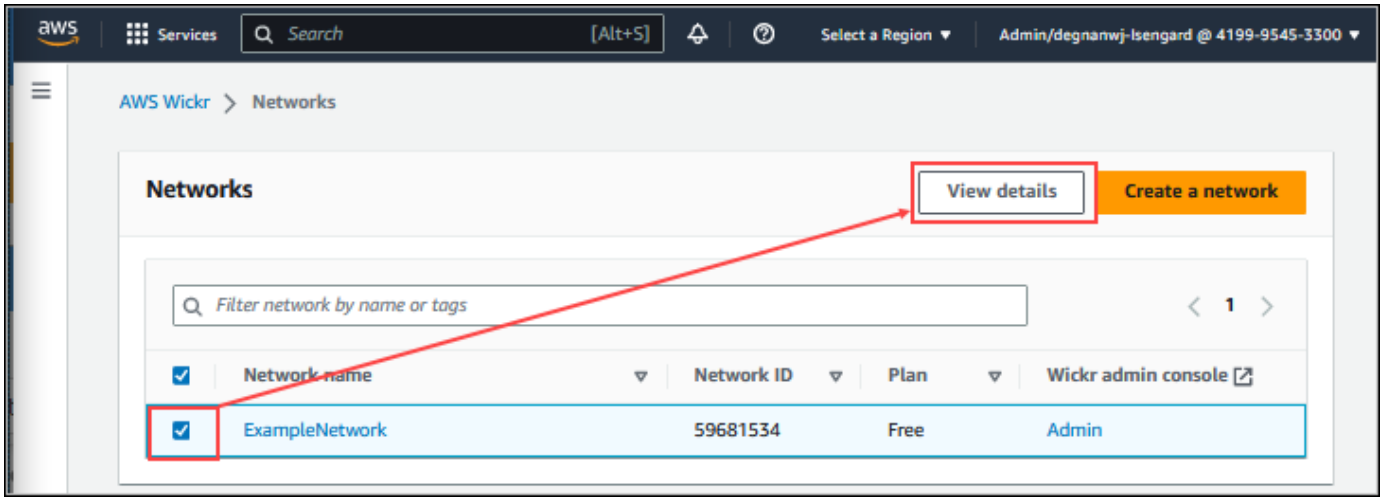
3. Wählen Sie im Navigationsbereich der Wickr Admin Console Netzwerkeinstellungen und dann Netzwerkprofil aus.

   Auf der Netzwerkprofilseite werden Ihr Wickr-Netzwerkname und Ihre Netzwerk-ID angezeigt. Sie können die Netzwerk-ID verwenden, um den Verbund zu konfigurieren.

Netzwerknamen bearbeiten

Gehen Sie wie folgt vor, um Ihren Wickr-Netzwerknamen zu bearbeiten.

1. Öffnen Sie AWS Management Console für Wickr Cat. https://console.aws.amazon.com/wickr/
2. Wählen Sie Netzwerk verwalten.
3. Aktivieren Sie auf der Seite Netzwerke das Kontrollkästchen neben dem Netzwerknamen, den Sie bearbeiten möchten, und wählen Sie dann Details anzeigen aus.



4. Wählen Sie im Abschnitt Netzwerkübersicht die Option Bearbeiten aus.
5. Geben Sie Ihren neuen Netzwerknamen in das Textfeld Netzwerkname ein.
6. Wählen Sie Änderungen speichern, um Ihren neuen Netzwerknamen zu speichern.

Sicherheitsgruppen

Im Bereich Sicherheitsgruppen der AWS Management Console für Wickr können Sie Sicherheitsgruppen und ihre Einstellungen verwalten, z. B. Richtlinien zur Kennwortkomplexität, Nachrichteneinstellungen, Anruffunktionen, Sicherheitsfunktionen und Netzwerkverbund.

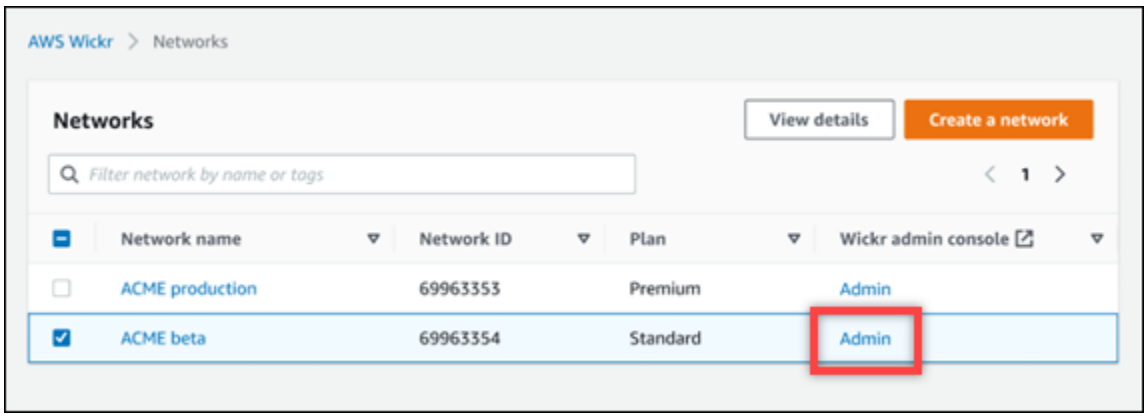
Themen

- Sicherheitsgruppen anzeigen
- Eine Sicherheitsgruppe erstellen
- Bearbeiten Sie eine Sicherheitsgruppe
- Löschen einer Sicherheitsgruppe

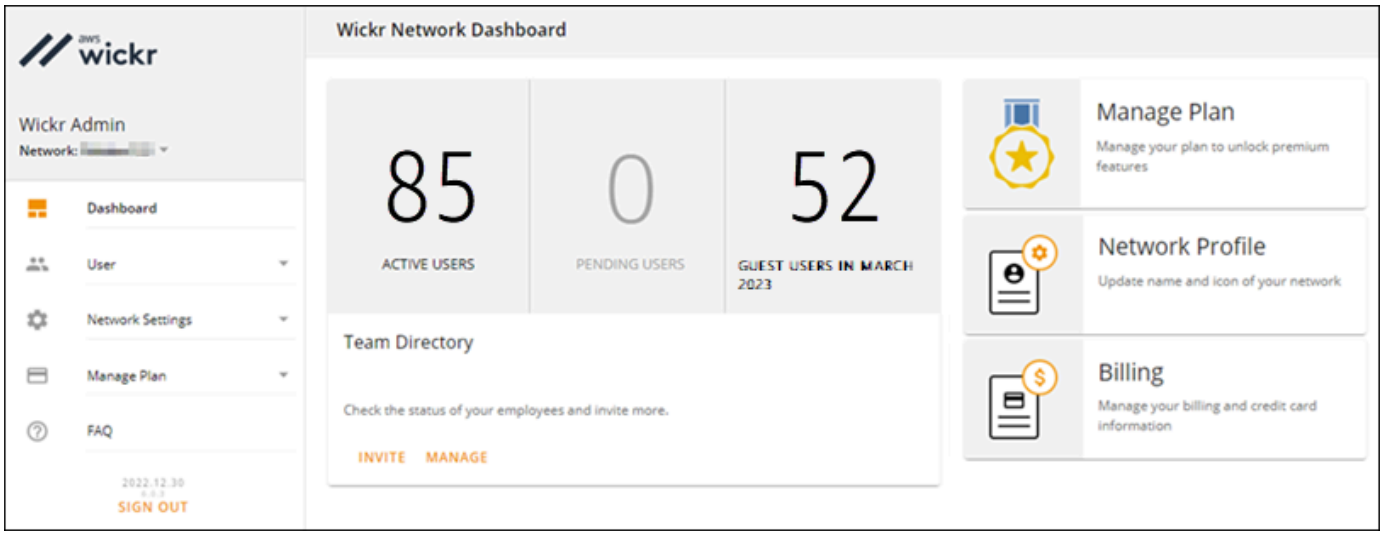
Sicherheitsgruppen anzeigen

Gehen Sie wie folgt vor, um Sicherheitsgruppen anzuzeigen.

1. Öffnen Sie AWS Management Console für Wickr Kat. https://console.aws.amazon.com/wickr/
2. Wählen Sie auf der Seite Netzwerke den Link Admin, um zur Wickr Admin Console für dieses Netzwerk zu gelangen.



Sie werden zur Wickr Admin Console für ein bestimmtes Netzwerk weitergeleitet.



3. Wählen Sie im Navigationsbereich der Wickr Admin Console Netzwerkeinstellungen und dann Sicherheitsgruppe aus.

   Auf der Seite Sicherheitsgruppen werden Ihre aktuellen Wickr-Sicherheitsgruppen angezeigt und Sie haben die Möglichkeit, deren Details einzusehen oder eine neue Gruppe zu erstellen.

Eine Sicherheitsgruppe erstellen

Gehen Sie wie folgt vor, um eine Sicherheitsgruppe zu erstellen.

1. Öffnen Sie AWS Management Console für Wickr Kat. https://console.aws.amazon.com/wickr/
2. Wählen Sie auf der Seite Netzwerke den Link Admin, um zur Wickr Admin Console für dieses Netzwerk zu gelangen.

   Sie werden zur Wickr Admin Console für ein bestimmtes Netzwerk weitergeleitet.

3. Wählen Sie im Navigationsbereich der Wickr Admin Console Netzwerkeinstellungen und dann Sicherheitsgruppe.
4. Wählen Sie Neue Gruppe, um eine neue Sicherheitsgruppe zu erstellen.

   Eine neue Sicherheitsgruppe mit einem Standardnamen wird automatisch zur Liste der Sicherheitsgruppen hinzugefügt.

   Weitere Informationen zum Bearbeiten der neuen Sicherheitsgruppe finden Sie unterBearbeiten Sie eine Sicherheitsgruppe.

Bearbeiten Sie eine Sicherheitsgruppe

Gehen Sie wie folgt vor, um eine Sicherheitsgruppe zu bearbeiten.

1. Öffnen Sie AWS Management Console für Wickr Kat. https://console.aws.amazon.com/wickr/
2. Wählen Sie auf der Seite Netzwerke den Link Admin, um zur Wickr Admin Console für dieses Netzwerk zu gelangen.

   Sie werden zur Wickr Admin Console für ein bestimmtes Netzwerk weitergeleitet.
3. Wählen Sie im Navigationsbereich der Wickr Admin Console Netzwerkeinstellungen und dann Sicherheitsgruppe.
4. Wählen Sie Details neben dem Namen der Sicherheitsgruppe, die Sie bearbeiten möchten.

   Auf der Seite mit den Sicherheitsgruppendetails werden die Einstellungen für die Sicherheitsgruppe auf verschiedenen Registerkarten angezeigt.
5. Die folgenden Registerkarten und die entsprechenden Einstellungen sind verfügbar:

   - Name der Sicherheitsgruppe — Wählen Sie das Stiftsymbol neben dem Namen der Gruppe, um den Namen zu bearbeiten.
   - Allgemein — Bearbeiten Sie die Grundkonfiguration der Gruppe.
   - Messaging — Verwaltet die Nachrichtenfunktionen für Mitglieder der Gruppe.
   - Telefonieren — Verwalten Sie die Anruffunktionen für Mitglieder der Gruppe.
   - Sicherheit — Konfigurieren Sie zusätzliche Sicherheitsfunktionen für die Gruppe.
   - Föderation — Die Fähigkeit, zwischen Netzwerken zu kommunizieren. Dies kann in der Admin-Konsole für ein Netzwerk auf Sicherheitsgruppenebene konfiguriert werden. AWSBei Wickr gibt es zwei Arten von Verbänden: lokal und global.

- Lokaler Verband — Die Fähigkeit, sich mit AWS Benutzern in anderen Netzwerken innerhalb derselben Region zu verbünden. Wenn es beispielsweise in Kanada zwei Netzwerke gibt, für die der lokale Verbund aktiviert ist, können sie miteinander kommunizieren.
- Globaler Verbund — Die Möglichkeit, sich entweder mit Enterprise-Benutzern zu verbünden oder AWS Benutzer in einem anderen Netzwerk, die zu anderen Regionen gehören. Wenn es beispielsweise einen Benutzer in einem Netzwerk in der Region Kanada und einen Benutzer in einem Netzwerk in der Region London gibt und der globale Verbund für beide Netzwerke aktiviert ist, können sie miteinander kommunizieren.
- Eingeschränkter Verbund — Die Möglichkeit, sich mit bestimmten Netzwerken zu verbinden (Enterprise oder AWS) gehören zu verschiedenen Regionen. Administratoren können bestimmte Netzwerke zulassen, mit denen sich ihre Benutzer verbünden können. Nach der Einschränkung können Benutzer nur mit Benutzern in den Netzwerken kommunizieren, die auf der Zulassungsliste stehen. Beide Netzwerke müssen sich in den Sicherheitsgruppeneinstellungen auf der Registerkarte Verbund gegenseitig auf eine Zulassungsliste setzen, um den eingeschränkten Verbund verwenden zu können.

6. Wählen Sie Speichern, um die Änderungen zu speichern, die Sie an den Sicherheitsgruppendetails vornehmen.

Löschen einer Sicherheitsgruppe

Gehen Sie wie folgt vor, um eine Sicherheitsgruppe zu löschen.

1. Öffnen Sie AWS Management Console für Wickr Kat. https://console.aws.amazon.com/wickr/
2. Wählen Sie auf der Seite Netzwerke den Link Admin, um zur Wickr Admin Console für dieses Netzwerk zu gelangen.

   Sie werden zur Wickr Admin Console für ein bestimmtes Netzwerk weitergeleitet.
3. Wählen Sie im Navigationsbereich der Wickr Admin Console Netzwerkeinstellungen und dann Sicherheitsgruppe.
4. Wählen Sie das vertikale Ellipsensymbol neben dem Namen der Sicherheitsgruppe, die Sie löschen möchten.
5. Wählen Sie Entfernen, um die Sicherheitsgruppe zu löschen.

   Wenn Sie eine Sicherheitsgruppe löschen, der Benutzer zugewiesen wurden, werden diese Benutzer automatisch der Standardsicherheitsgruppe hinzugefügt. Informationen zum Ändern der den Benutzern zugewiesenen Sicherheitsgruppe finden Sie unterBenutzer bearbeiten.

Konfiguration von Single Sign-On

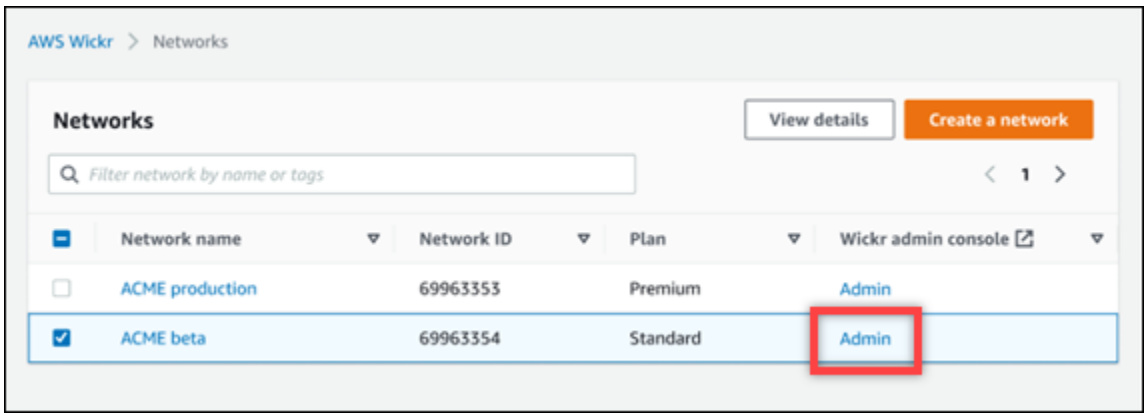
Im Abschnitt SSOKonfiguration des AWS Management Console für Wickr können Sie Wickr so konfigurieren, dass es ein Single-Sign-On-System zur Authentifizierung verwendet. SSObietet in Kombination mit einem geeigneten Multi-Faktor-Authentifizierungssystem () eine zusätzliche Sicherheitsebene. MFA Wickr unterstützt nur SSO Anbieter, die OpenID Connect (OIDC) verwenden. Anbieter, die Security Assertion Markup Language (SAML) verwenden, werden nicht unterstützt.

Themen

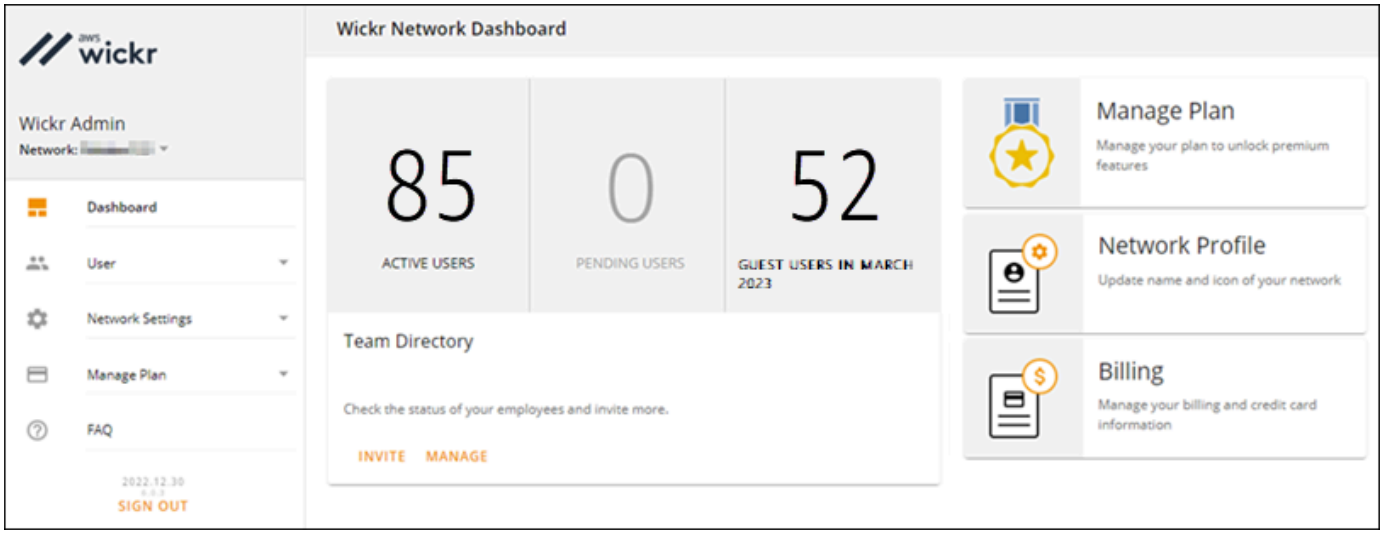
Einzelheiten anzeigen SSO

Gehen Sie wie folgt vor, um die aktuelle Single Sign-On-Konfiguration für Ihr Wickr-Netzwerk anzuzeigen, falls vorhanden. Sie können auch den Netzwerkendpunkt für Ihr Wickr-Netzwerk anzeigen.

1. Öffnen Sie AWS Management Console für Wickr bei. https://console.aws.amazon.com/wickr/
2. Wählen Sie auf der Seite Netzwerke den Link Admin, um zur Wickr Admin Console für dieses Netzwerk zu gelangen.



   Sie werden zur Wickr Admin Console für ein bestimmtes Netzwerk weitergeleitet.



3. Wählen Sie im Navigationsbereich der Wickr Admin Console Netzwerkeinstellungen und dann SSOKonfiguration.

   Auf der Seite Single Sign-On & LDAP Configuration werden Ihr Wickr-Netzwerkendpunkt und die aktuelle Konfiguration angezeigt. SSO

Konfigurieren SSO

Weitere Informationen zur Konfiguration finden SSO Sie in den folgenden Anleitungen:

> **Important**
>
> Bei der Konfiguration SSO geben Sie eine Unternehmens-ID für Ihr Wickr-Netzwerk an. Notieren Sie sich unbedingt die Firmen-ID für Ihr Wickr-Netzwerk. Sie müssen es Ihren Endbenutzern beim Versenden von Einladungs-E-Mails zur Verfügung stellen. Endbenutzer müssen die Unternehmens-ID angeben, wenn sie sich für Ihr Wickr-Netzwerk registrieren.

- Microsoft Entra (Azure AD) Single Sign-On konfigurieren
- Konfigurieren Sie Okta Single Sign-On

Übergangsfrist für die Token-Aktualisierung

Gelegentlich kann es vorkommen, dass Identitätsanbieter auf vorübergehende oder längere Ausfälle stoßen, was dazu führen kann, dass Ihre Benutzer aufgrund eines fehlgeschlagenen

Aktualisierungstokens für ihre Clientsitzung unerwartet abgemeldet werden. Um dieses Problem zu vermeiden, können Sie eine Übergangsfrist einrichten, die es Ihren Benutzern ermöglicht, angemeldet zu bleiben, auch wenn ihr Client-Aktualisierungstoken bei solchen Ausfällen ausfällt.

Hier sind die verfügbaren Optionen für den Kulanzzeitraum:

- Keine Kulanzfrist (Standard): Benutzer werden sofort nach einem Fehler bei einem Aktualisierungstoken abgemeldet.
- Nachfrist von 30 Minuten: Benutzer können bis zu 30 Minuten angemeldet bleiben, nachdem ein Aktualisierungstoken fehlgeschlagen ist.
- Kulanzzeit von 60 Minuten: Benutzer können nach einem Fehler beim Aktualisierungstoken bis zu 60 Minuten angemeldet bleiben.

Microsoft Entra (Azure AD) Single Sign-On konfigurieren

AWSWickr kann so konfiguriert werden, dass Microsoft Entra (Azure AD) als Identitätsanbieter verwendet wird. Führen Sie dazu die folgenden Verfahren sowohl in Microsoft Entra als auch in der AWS Wickr-Administrationskonsole aus.

> **Warning**
>
> Nach SSO der Aktivierung in einem Netzwerk werden aktive Benutzer von Wickr abgemeldet und sie werden gezwungen, sich über den Anbieter erneut zu authentifizieren. SSO

Schritt 1: AWS Wickr als Anwendung in Microsoft Entra registrieren

Gehen Sie wie folgt vor, um AWS Wickr als Anwendung in Microsoft Entra zu registrieren.

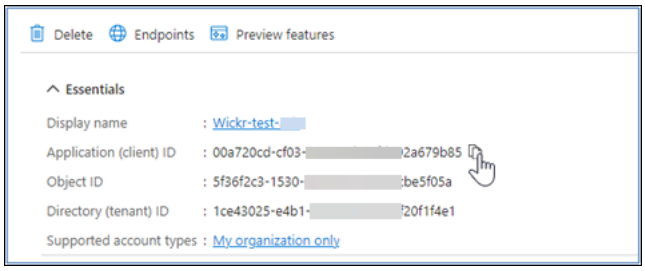
> **Note**
>
> Detaillierte Screenshots und Problemlösungen finden Sie in der Microsoft Entra-Dokumentation. Weitere Informationen finden Sie unter Registrieren einer Anwendung bei der Microsoft Identity Platform

1. Wählen Sie im Navigationsbereich Anwendungen und dann App-Registrierungen aus.

2. Wählen Sie auf der Seite App-Registrierungen die Option Anwendung registrieren aus und geben Sie dann einen Anwendungsnamen ein.
3. Wählen Sie Nur Konten in diesem Organisationsverzeichnis aus (Nur Standardverzeichnis — Einzelmandant).
4. Wählen Sie unter Umleitung die Option Web ausURI, und geben Sie dann die folgende Webadresse ein:`https://messaging-pro-prod.wickr.com/deeplink/oidc.php`.

> **Note**
>
> Die Umleitung URI kann auch aus den SSO Konfigurationseinstellungen in der AWS Wickr Admin-Konsole kopiert werden.

5. Wählen Sie Register aus.
6. Kopieren/speichern Sie nach der Registrierung die generierte Anwendungs-ID (Client).



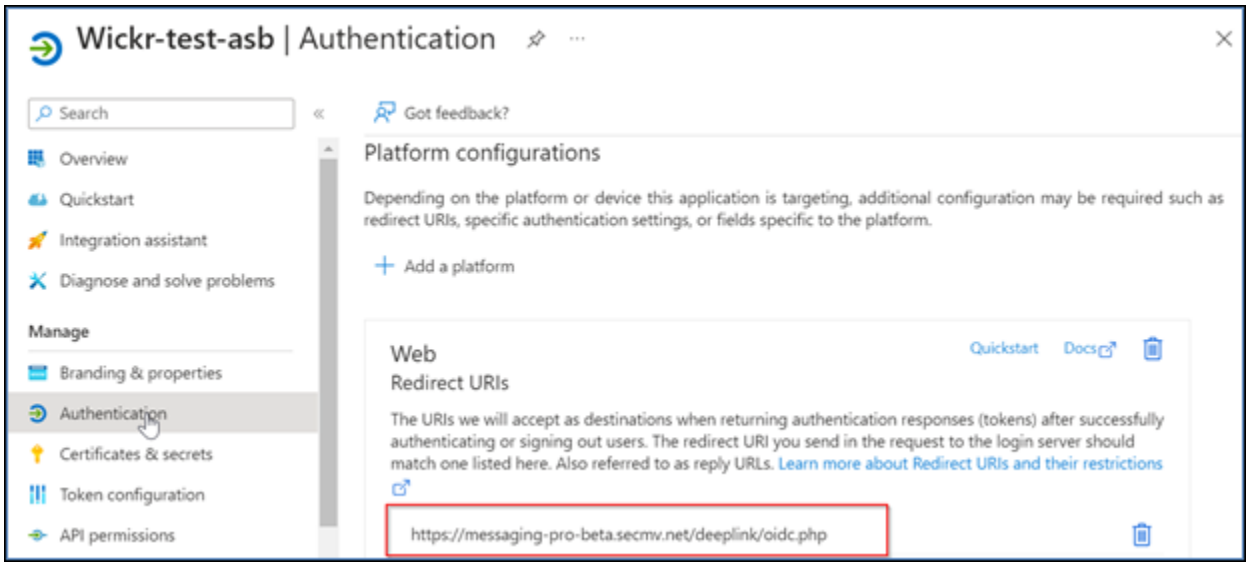
7. Wählen Sie die Registerkarte Endpoints, um sich Folgendes zu notieren:
   1. OAuth 2.0-Autorisierungsendpunkt (v2): z. B.: `https://login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/oauth2/v2.0/authorize`
   2. Bearbeiten Sie diesen Wert, um „oauth2/“ und „authorize“ zu entfernen. Zum Beispiel wird fixed so aussehenURL: `https://login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/v2.0/`
   3. Dieser wird als SSOEmittent bezeichnet.

Schritt 2: Authentifizierung einrichten

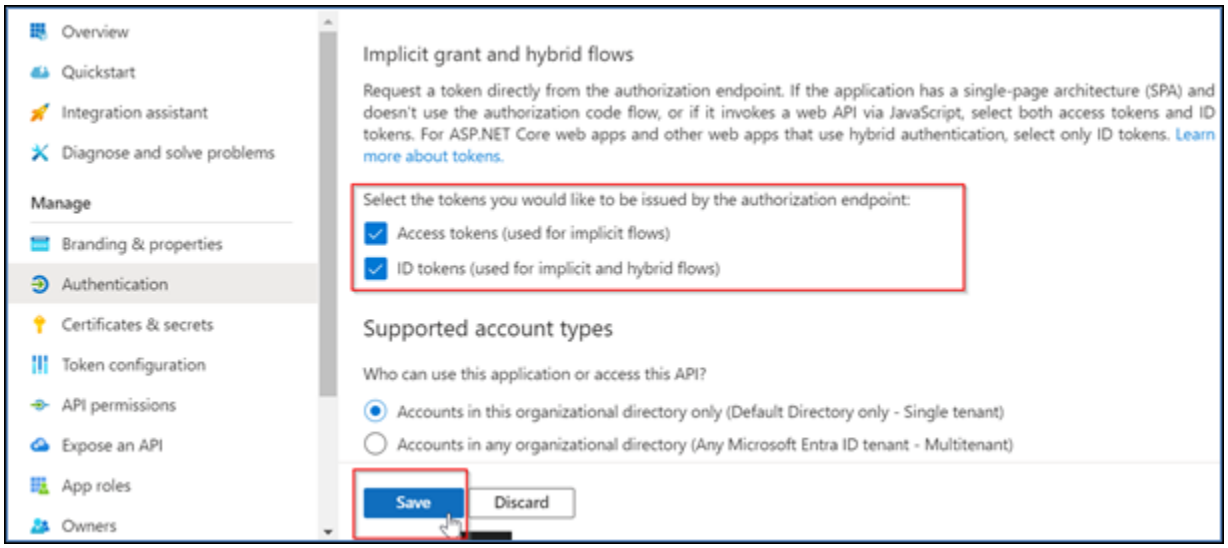
Gehen Sie wie folgt vor, um die Authentifizierung in Microsoft Entra einzurichten.

1. Wählen Sie im Navigationsbereich Authentifizierung aus.

2. Stellen Sie auf der Authentifizierungsseite sicher, dass die Web-Umleitung dieselbe URI ist, die Sie zuvor eingegeben haben (unter AWSWickr als Anwendung registrieren).



3. Wählen Sie Zugriffstoken aus, die für implizite Datenflüsse verwendet werden, und ID-Token, die für implizite und hybride Datenflüsse verwendet werden.
4. Wählen Sie Save (Speichern) aus.

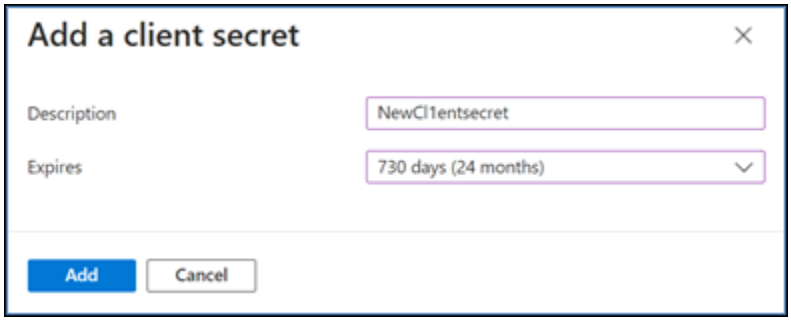


Schritt 3: Zertifikate und Geheimnisse einrichten

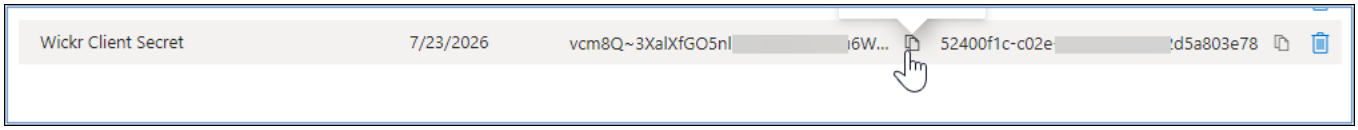
Gehen Sie wie folgt vor, um Zertifikate und Geheimnisse in Microsoft Entra einzurichten.

1. Wählen Sie im Navigationsbereich Certificates & Secrets aus.
2. Wählen Sie auf der Seite Certificates & Secrets die Registerkarte Client Secrets aus.

3. Wählen Sie auf der Registerkarte Client-Geheimnisse die Option Neues Client-Geheimnis aus.
4. Geben Sie eine Beschreibung ein und wählen Sie einen Ablaufzeitraum für das Geheimnis aus.
5. Wählen Sie Hinzufügen aus.



6. Kopieren Sie nach der Erstellung des Zertifikats den Wert für den geheimen Clientschlüssel.

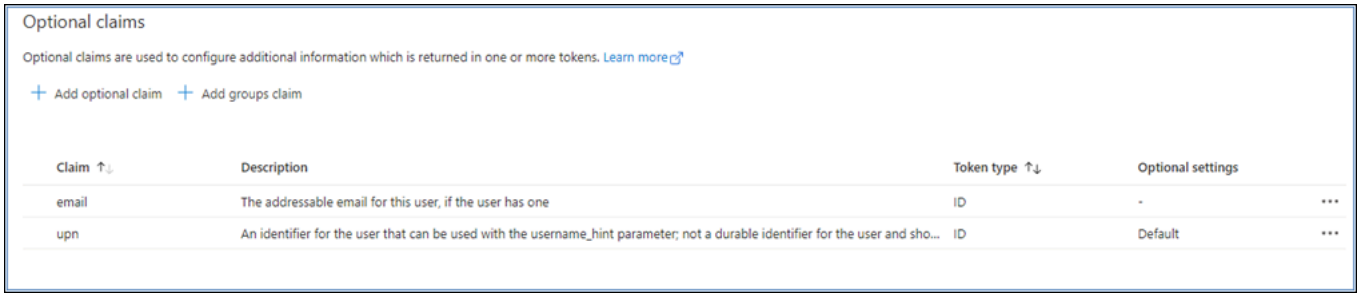


> **Note**
>
> Der geheime Wert des Client (nicht Secret ID) wird für Ihren Client-Anwendungscode benötigt. Möglicherweise können Sie den geheimen Wert nicht anzeigen oder kopieren, nachdem Sie diese Seite verlassen haben. Wenn Sie ihn jetzt nicht kopieren, müssen Sie zurückgehen, um einen neuen geheimen Clientschlüssel zu erstellen.

Schritt 4: Token-Konfiguration einrichten

Gehen Sie wie folgt vor, um die Tokenkonfiguration in Microsoft Entra einzurichten.

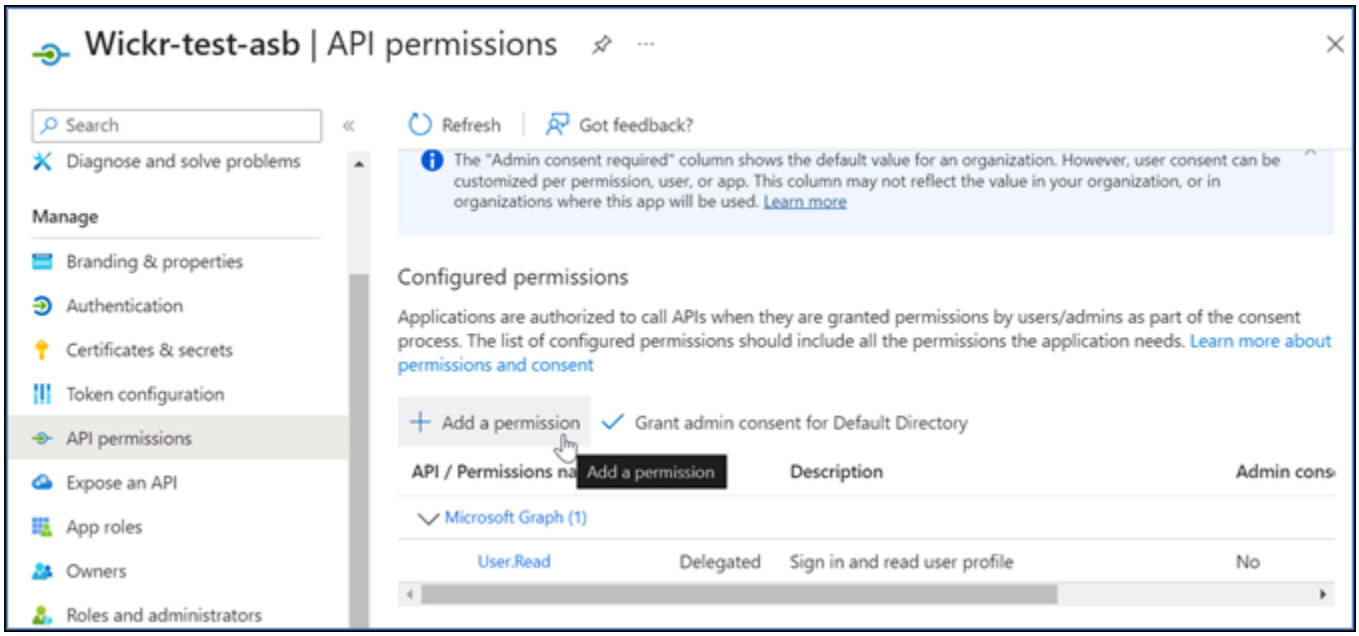
1. Wählen Sie im Navigationsbereich Tokenkonfiguration aus.
2. Wählen Sie auf der Seite Token-Konfiguration die Option Optionalen Anspruch hinzufügen aus.
3. Wählen Sie unter Optionale Ansprüche den Token-Typ als ID aus.
4. Nachdem Sie ID ausgewählt haben, wählen Sie unter Anspruch die Option E-Mail und UPN aus.
5. Wählen Sie Hinzufügen aus.



Schritt 5: API Berechtigungen einrichten

Gehen Sie wie folgt vor, um API Berechtigungen in Microsoft Entra einzurichten.

1. Wählen Sie im Navigationsbereich APIBerechtigungen aus.
2. Wählen Sie auf der Seite mit den APIBerechtigungen die Option Berechtigung hinzufügen aus.



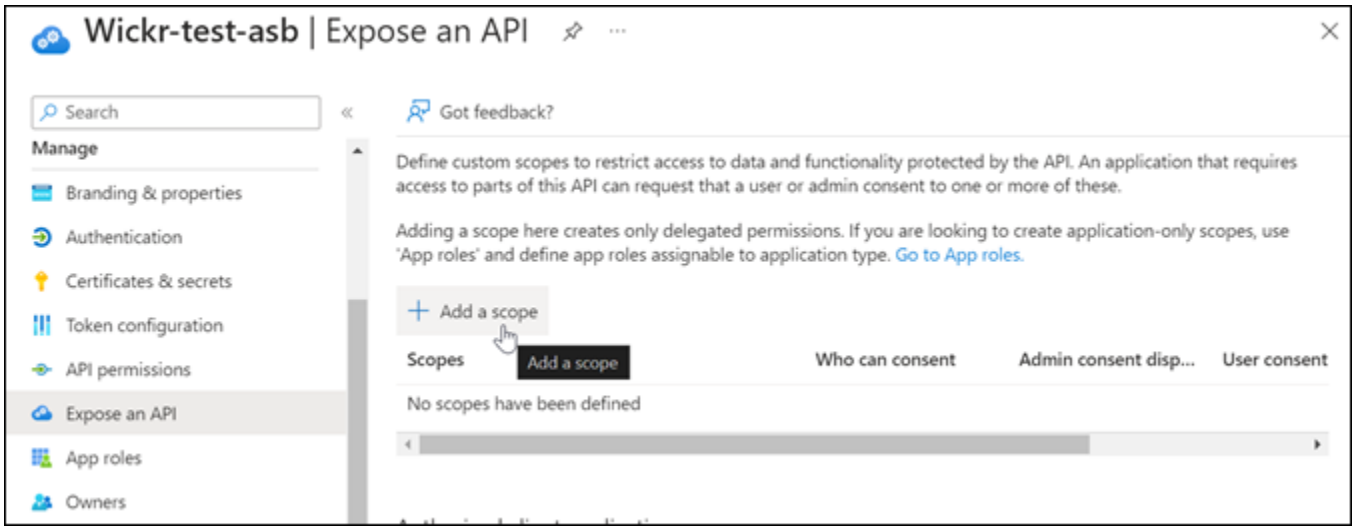
3. Wählen Sie Microsoft Graph und dann Delegierte Berechtigungen aus.
4. Aktivieren Sie das Kontrollkästchen für E-Mail, Offline_Access, OpenID und Profil.
5. Wählen Sie Add permissions (Berechtigungen hinzufügen) aus.

Schritt 6: Enthüllen Sie eine API

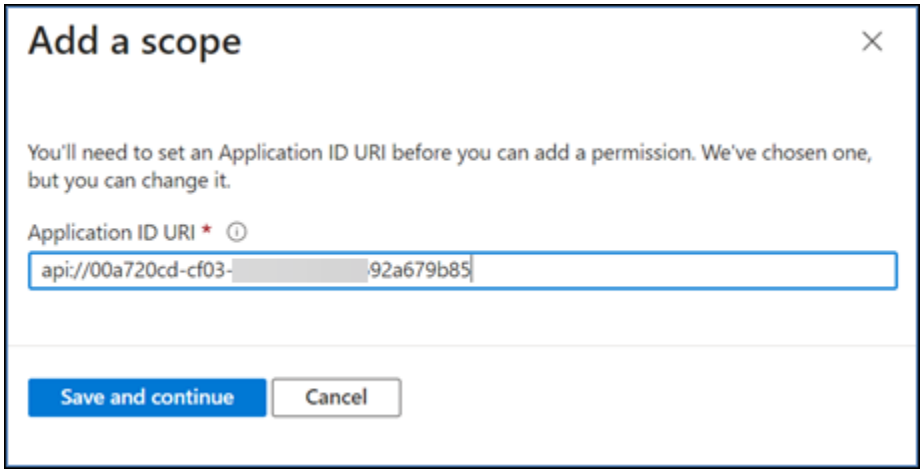
Gehen Sie wie folgt vor, um API für jeden der 4 Bereiche in Microsoft Entra eine verfügbar zu machen.

1. Wählen Sie im Navigationsbereich die Option Expose an aus. API

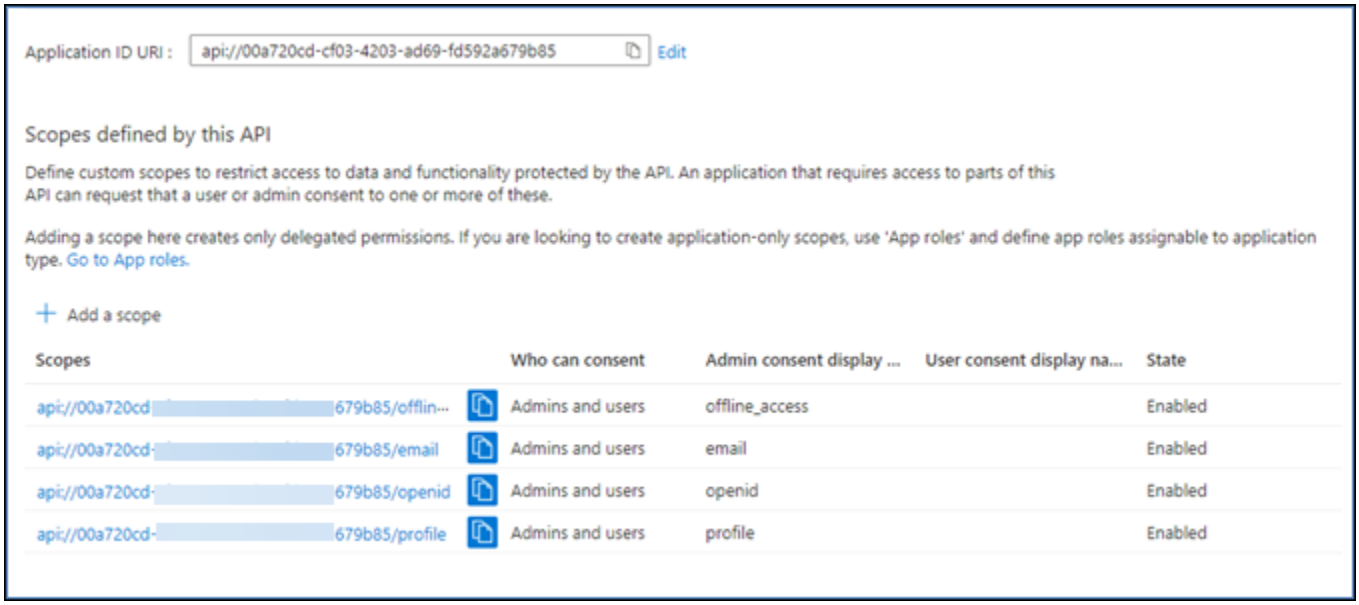
2. Wählen Sie auf der API Seite „Einen Bereich anzeigen“ die Option Bereich hinzufügen aus.



Die Anwendungs-ID URI sollte auto ausgefüllt werden, und die ID, die auf die folgt, URI sollte mit der Anwendungs-ID übereinstimmen (erstellt in AWSWickr als Anwendung registrieren).



3. Wählen Sie Save and continue aus.
4. Wählen Sie das Tag Admins and users aus und geben Sie dann den Bereichsnamen als offline_access ein.
5. Wählen Sie Status und dann Aktivieren aus.
6. Wählen Sie Bereich hinzufügen aus.
7. Wiederholen Sie die Schritte 1—6 dieses Abschnitts, um die folgenden Bereiche hinzuzufügen: E-Mail, OpenID und Profil.



8. Wählen Sie unter Autorisierte Clientanwendungen die Option Clientanwendung hinzufügen aus.
9. Wählen Sie alle vier Bereiche aus, die im vorherigen Schritt erstellt wurden.
10. Geben Sie die Anwendungs-ID (Client) ein oder überprüfen Sie sie.
11. Wählen Sie Anwendung hinzufügen.

Schritt 7: AWS Wickr-Konfiguration SSO

Schließen Sie das folgende Konfigurationsverfahren in der AWS Wickr-Konsole ab.

1. Öffnen Sie AWS Management Console für Wickr Cat. https://console.aws.amazon.com/wickr/
2. Wählen Sie auf der Seite Netzwerke den Link Admin, um zur Wickr Admin Console für dieses Netzwerk zu navigieren.
3. Wählen Sie im Navigationsbereich der Wickr Admin Console Netzwerkeinstellungen und dann Konfiguration. SSO
4. Stellen Sie unter Netzwerkendpunkt sicher, dass die Weiterleitung URI mit der folgenden Webadresse übereinstimmt (in Schritt 4 unter AWSWickr als Anwendung registrieren hinzugefügt).

   `https://messaging-pro-prod.wickr.com/deeplink/oidc.php`.
5. Wählen Sie unter SSOKonfiguration die Option Start
6. Geben Sie die folgenden Details ein:

- SSOEmittent — Dies ist der Endpunkt, der zuvor geändert wurde (z. B.`https://login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/v2.0/`).
- SSOClient-ID — Dies ist die Anwendungs-ID (Client) aus dem Übersichtsbereich.
- Unternehmens-ID — Dies kann ein eindeutiger Textwert sein, der alphanumerische Zeichen und Unterstriche enthält. Dieser Satz wird von Ihren Benutzern eingegeben, wenn sie sich auf neuen Geräten registrieren.
- Geheimer Client — Dies ist der geheime Client-Schlüssel aus dem Bereich Certificates & Secrets.
- Bereiche — Dies sind die Bereichsnamen, die im API Bereich Offenlegen angezeigt werden. Geben Sie email, profile, offline_access und openid ein.
- Benutzerdefinierter Benutzernamenbereich — Geben Sie upn ein.

Andere Felder sind optional.

7. Wählen Sie Testen und Speichern.
8. Wählen Sie Save (Speichern) aus.

SSODie Konfiguration ist abgeschlossen. Zur Überprüfung können Sie der Anwendung in Microsoft Entra jetzt einen Benutzer hinzufügen und sich mit dem Benutzer anmelden, der eine Unternehmens-ID verwendetSSO.

Weitere Informationen zum Einladen und Einbinden von Benutzern finden Sie unter Benutzer erstellen und einladen.

Fehlerbehebung

Im Folgenden finden Sie häufig auftretende Probleme und Lösungsvorschläge.

- SSODer Verbindungstest schlägt fehl oder reagiert nicht:
  - Stellen Sie sicher, dass der SSOAussteller wie erwartet konfiguriert ist.
  - Stellen Sie sicher, dass die erforderlichen Felder im Feld SSOKonfiguriert wie erwartet festgelegt sind.
- Der Verbindungstest ist erfolgreich, aber der Benutzer kann sich nicht anmelden:
  - Stellen Sie sicher, dass der Benutzer zu der Wickr-Anwendung hinzugefügt wurde, die Sie in Microsoft Entra registriert haben.

- Stellen Sie sicher, dass der Benutzer die richtige Unternehmens-ID einschließlich des Präfixes verwendet. Z.B. UE1- DemoNetwork w_DRATVA.
- Das Client Secret ist in der Wickr-Konfiguration möglicherweise nicht korrekt eingestellt. AWS SSO Setzen Sie es zurück, indem Sie ein anderes Client-Geheimnis in Microsoft Entra erstellen und das neue Client-Geheimnis in der SSOWickr-Konfiguration festlegen.

Quittungen lesen

Lesebestätigungen auf Wickr sind Benachrichtigungen, die an den Absender gesendet werden, um anzuzeigen, wann seine Nachricht gelesen wurde. Diese Belege sind in Konversationen verfügbar. one-on-one Für gesendete Nachrichten wird ein einzelnes Häkchen und für gelesene Nachrichten ein durchgezogener Kreis mit einem Häkchen angezeigt. Um Lesebestätigungen für Nachrichten während externer Konversationen zu sehen, sollten Lesebestätigungen in beiden Netzwerken aktiviert sein.

Administratoren können Lesebestätigungen im Administratorbereich aktivieren oder deaktivieren. Diese Einstellung wird auf das gesamte Netzwerk angewendet.

Gehen Sie wie folgt vor, um Lesebestätigungen zu aktivieren oder zu deaktivieren.

1. Öffnen Sie AWS Management Console für Wickr Kat. https://console.aws.amazon.com/wickr/
2. Wählen Sie im Navigationsbereich der Wickr Admin Console Netzwerkeinstellungen und dann Netzwerkprofil aus.
3. Wählen Sie auf der Netzwerkprofilseite im Abschnitt Lesebestätigungen die Option Bearbeiten aus.
4. Wählen Sie Aktivieren oder Deaktivieren aus.

Netzwerk-Tags

Sie können Tags auf Wickr-Netzwerke anwenden. Sie können diese Tags dann verwenden, um Ihre Wickr-Netzwerke zu suchen und zu filtern oder Ihre AWS Kosten. Sie können Netzwerk-Tags auf der Netzwerkübersichtsseite des konfigurieren AWS Management Console für Wickr.

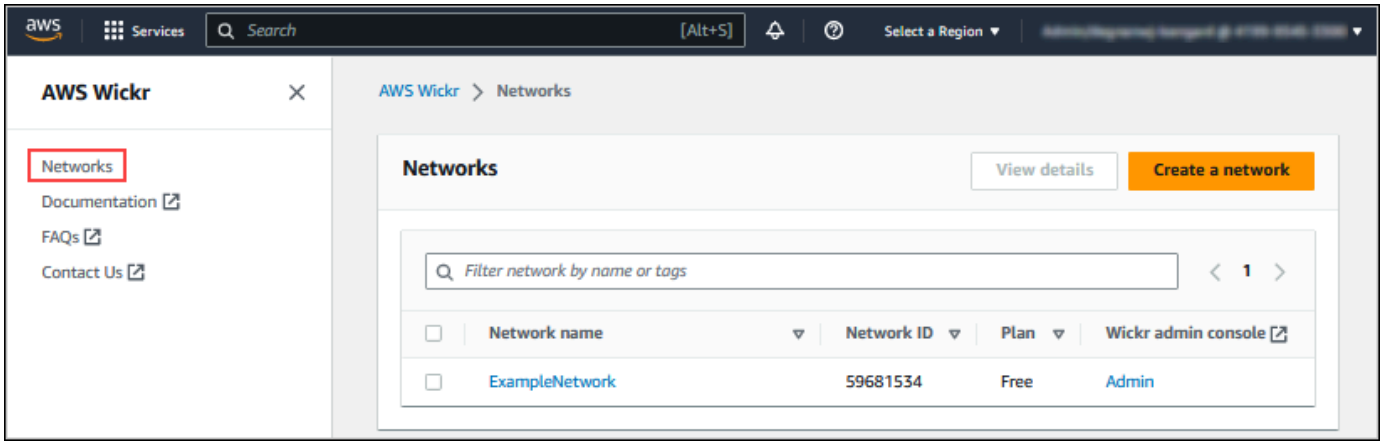
Ein Tag ist ein Schlüssel-Wert-Paar, das auf eine Ressource angewendet wird und Metadaten zu dieser Ressource enthält. Jedes Tag ist eine Bezeichnung, die aus einem Schlüssel und einem Wert

besteht. Weitere Informationen zu Tags finden Sie auch unter Was sind Tags? und Anwendungsfälle zum Taggen.

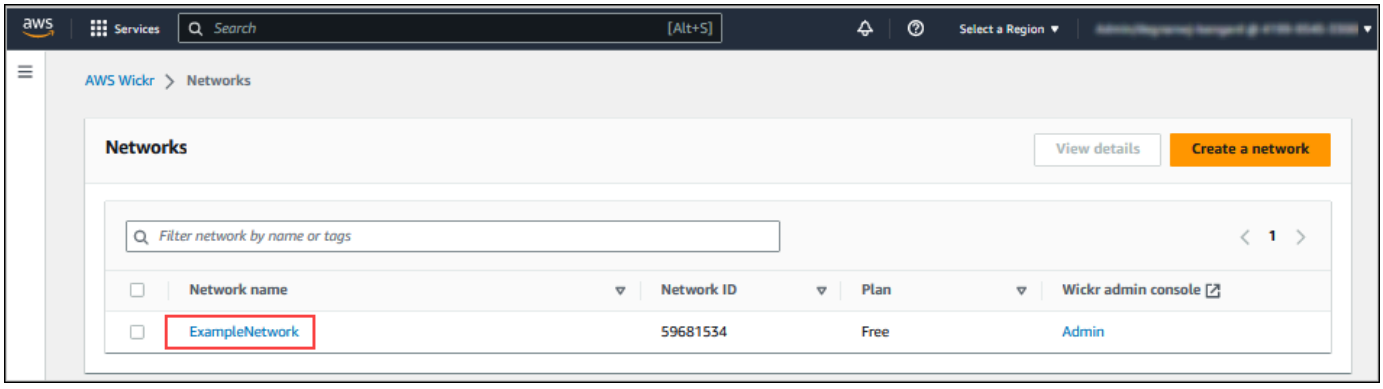
Netzwerk-Tags verwalten

Gehen Sie wie folgt vor, um Netzwerk-Tags für Ihr Wickr-Netzwerk zu verwalten.

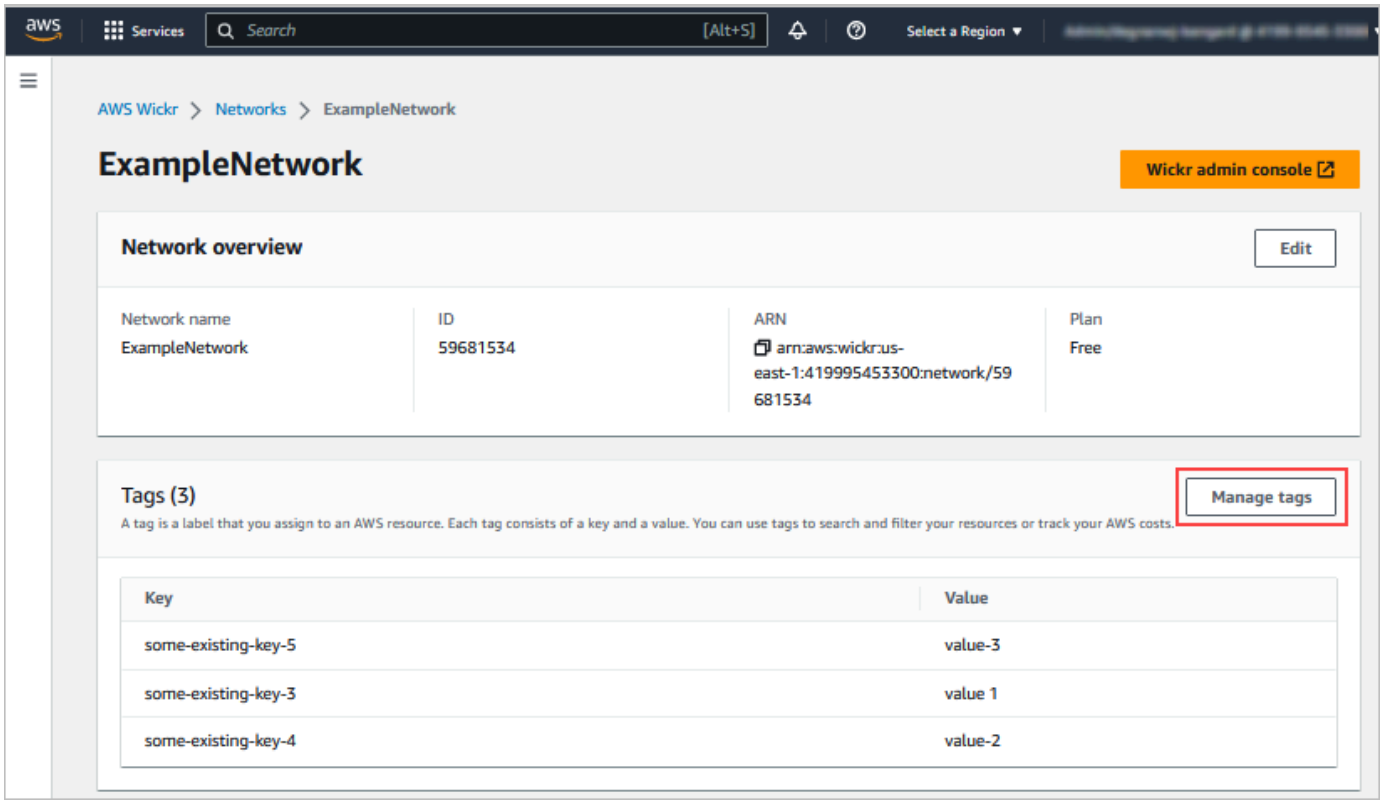
1. Öffnen Sie AWS Management Console für Wickr Cat. https://console.aws.amazon.com/wickr/
2. Wählen Sie Netzwerke im Navigationsbereich des AWS Management Console für Wickr.



3. Wählen Sie auf der Seite Netzwerke den Namen des Netzwerks aus, für das Sie Tags verwalten möchten.



4. Wählen Sie auf der Netzwerkübersichtsseite die Option Tags verwalten aus.



5. Auf der Seite „Tags verwalten“ können Sie eine der folgenden Optionen auswählen:

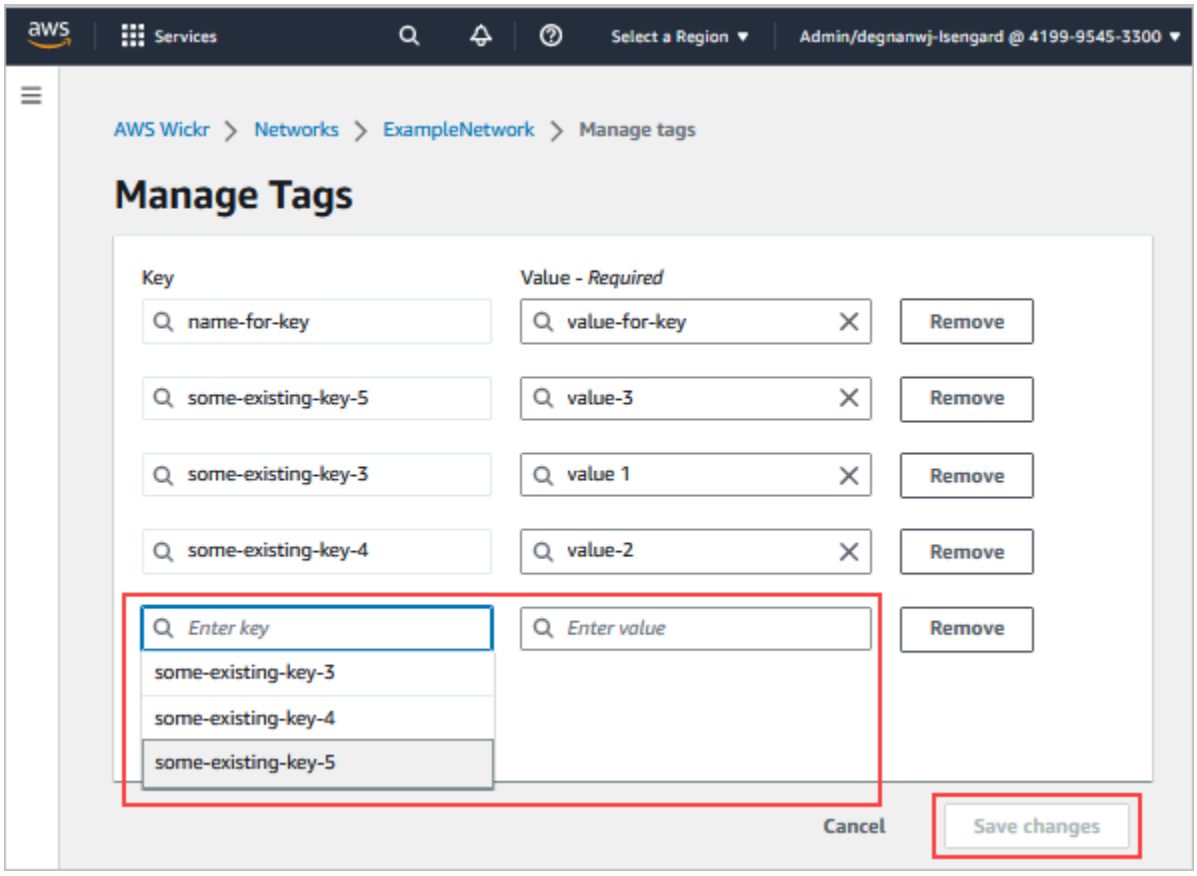
   - Neue Tags hinzufügen — Geben Sie neue Tags in Form eines Schlüssel- und Wertepaars ein. Wählen Sie Neues Tag hinzufügen, um mehrere Schlüssel-Wert-Paare hinzuzufügen. Bei Tags muss die Groß- und Kleinschreibung beachtet werden. Weitere Informationen finden Sie unter Fügen Sie ein Netzwerk-Tag hinzu.
   - Bestehende Tags bearbeiten — Wählen Sie den Schlüssel- oder Werttext für ein vorhandenes Tag aus und geben Sie dann die Änderung in das Textfeld ein. Weitere Informationen finden Sie unter Bearbeiten Sie ein Netzwerk-Tag.
   - Bestehende Tags entfernen — Wählen Sie die Schaltfläche Entfernen, die neben dem Tag aufgeführt ist, den Sie löschen möchten. Weitere Informationen finden Sie unter Entfernen Sie ein Netzwerk-Tag.

Fügen Sie ein Netzwerk-Tag hinzu

Gehen Sie wie folgt vor, um Ihrem Wickr-Netzwerk ein Tag hinzuzufügen. Weitere Informationen zur Verwaltung von Tags finden Sie unterNetzwerk-Tags verwalten.

1. Wählen Sie auf der Seite Tags verwalten Neuen Tag hinzufügen aus.

2. Geben Sie in die leeren Felder Schlüssel und Wert, die nun angezeigt werden, den Schlüssel und den Wert des neuen Tags ein.
3. Wählen Sie Änderungen speichern, um die neuen Tags zu speichern.

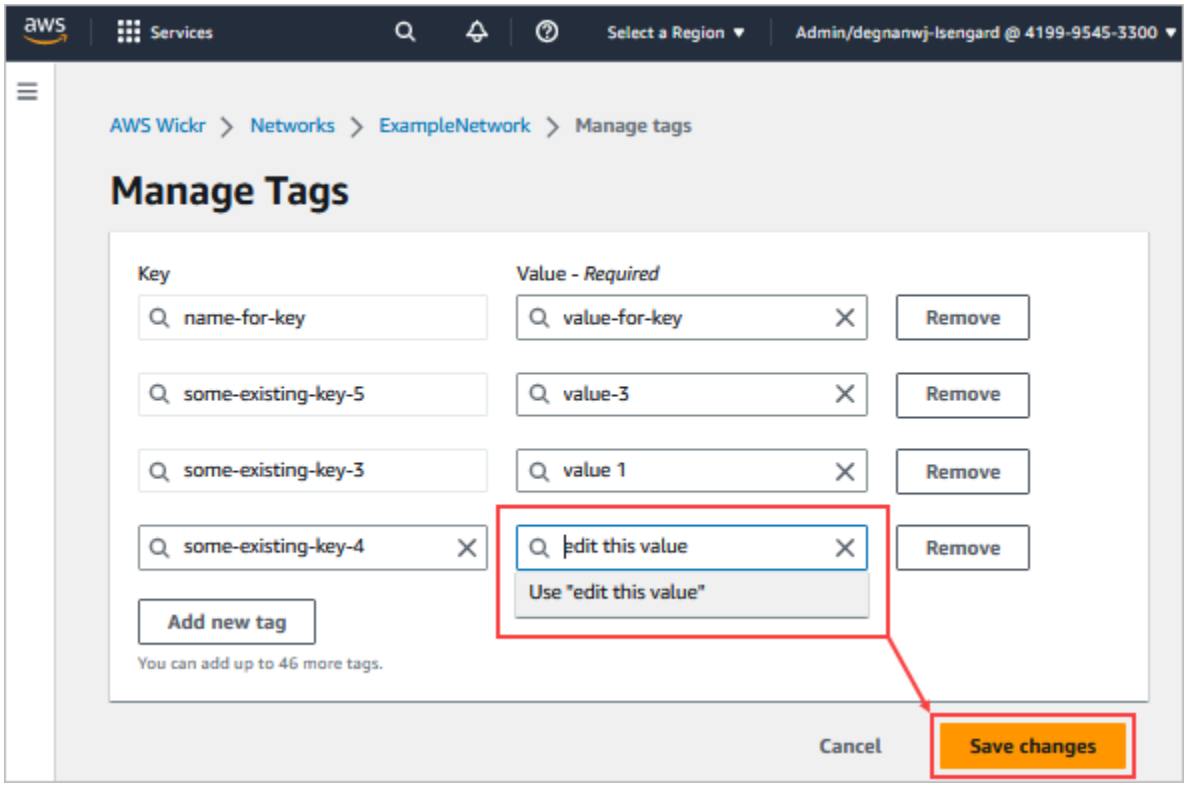


Bearbeiten Sie ein Netzwerk-Tag

Gehen Sie wie folgt vor, um ein mit Ihrem Wickr-Netzwerk verknüpftes Tag zu bearbeiten. Weitere Informationen zur Verwaltung von Tags finden Sie unterNetzwerk-Tags verwalten.

1. Bearbeiten Sie auf der Seite „Tags verwalten“ den Wert eines Tags.

> **Note**
>
> Sie können den Schlüssel eines Tags nicht bearbeiten. Entfernen Sie stattdessen das Schlüssel- und Wertepaar und fügen Sie mithilfe des neuen Schlüssels ein neues Tag hinzu.

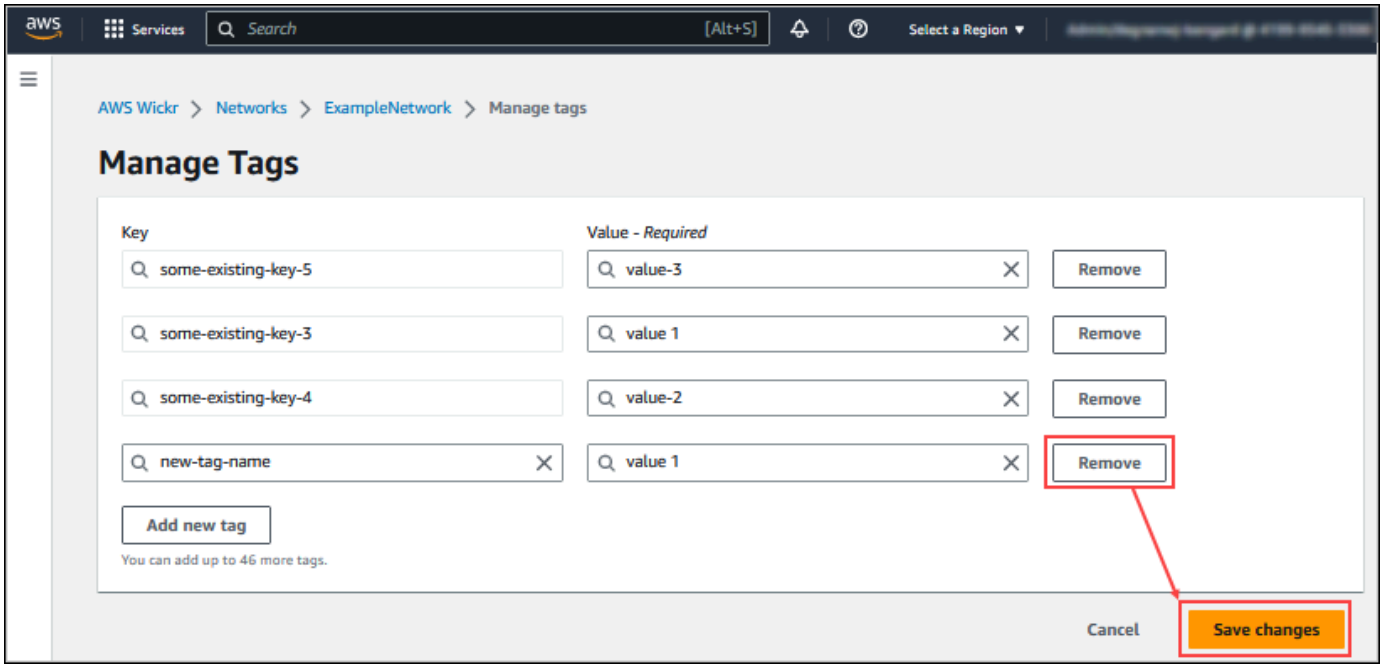


2. Wählen Sie Änderungen speichern, um Ihre Änderungen zu speichern.

Entfernen Sie ein Netzwerk-Tag

Gehen Sie wie folgt vor, um ein Tag aus Ihrem Wickr-Netzwerk zu entfernen. Weitere Informationen zur Verwaltung von Tags finden Sie unterNetzwerk-Tags verwalten.

1. Wählen Sie auf der Seite „Stichwörter verwalten“ für das Tag, das Sie entfernen möchten, die Option Entfernen aus.



2. Wählen Sie Änderungen speichern, um Ihre Änderungen zu speichern.

Netzwerkplan verwalten

Im Abschnitt „Plan verwalten“ der AWS Management Console für Wickr können Sie Ihren Netzwerkplan auf der Grundlage Ihrer Geschäftsanforderungen verwalten.

Gehen Sie wie folgt vor, um Ihren Netzwerkplan zu verwalten.

1. Öffnen Sie AWS Management Console für Wickr Kat. https://console.aws.amazon.com/wickr/
2. Wählen Sie im Navigationsbereich der Wickr Admin Console die Option Plan verwalten und dann Mein Plan aus.
3. Wählen Sie auf der Seite Mein Plan den gewünschten Netzwerkplan aus. Sie können Ihren aktuellen Netzwerkplan ändern, indem Sie einen der folgenden Optionen wählen:

   - Standard — Für kleine und große Unternehmensteams, die administrative Kontrollen und Flexibilität benötigen.
   - Premium - oder kostenlose Premium-Testversion — Für Unternehmen, die höchste Funktionseinschränkungen, detaillierte Verwaltungskontrollen und Datenspeicherung benötigen.

     Administratoren können die kostenlose Premium-Testoption wählen, die für bis zu 30 Benutzer verfügbar ist und drei Monate gültig ist. Dieses Angebot gilt für neue, legacy-

freie Testversionen und Standardpläne. Administratoren können während der kostenlosen Premium-Testphase ein Upgrade oder Downgrade auf Premium- oder Standard-Tarife durchführen.

> **Note**
>
> Um die Nutzung und Abrechnung in Ihrem Netzwerk zu beenden, entfernen Sie alle Benutzer, einschließlich aller gesperrten Benutzer, aus Ihrem Netzwerk.

Einschränkungen der kostenlosen Premium-Testversion

Die folgenden Einschränkungen gelten für die kostenlose Premium-Testversion:

- Wenn ein Plan schon einmal für eine kostenlose Premium-Testversion registriert wurde, ist er nicht für eine weitere Testversion berechtigt.
- Nur ein Netzwerk für jedes AWS Das Konto kann für eine kostenlose Premium-Testversion registriert werden.
- Die Gastbenutzerfunktion ist während der kostenlosen Premium-Testversion nicht verfügbar.
- Wenn ein Standardnetzwerk mehr als 30 Benutzer hat, ist ein Upgrade auf eine kostenlose Premium-Testversion nicht möglich.

Datenaufbewahrung

AWSMit Wickr Data Retention können alle Konversationen im Netzwerk gespeichert werden. Dazu gehören Direktnachrichtengespräche und Konversationen in Gruppen oder Räumen zwischen (internen) Mitgliedern im Netzwerk und denen mit anderen Teams (extern), mit denen Ihr Netzwerk verbunden ist. Die Datenspeicherung ist nur für Benutzer des AWS Wickr Premium-Tarifs und Unternehmenskunden verfügbar, die sich für die Datenspeicherung entscheiden. Weitere Informationen zum Premium-Plan finden Sie unter Wickr Pricing

Wenn ein Netzwerkadministrator die Datenspeicherung für sein Netzwerk konfiguriert und aktiviert, werden alle Nachrichten und Dateien, die in seinem Netzwerk geteilt werden, gemäß den Compliance-Richtlinien des Unternehmens aufbewahrt. Auf diese TXT-Dateiausgaben kann der Netzwerkadministrator an einem externen Ort zugreifen (z. B. lokaler Speicher, Amazon S3 S3-Bucket oder ein anderer Speicher nach Wahl des Benutzers), von wo aus sie analysiert, gelöscht oder übertragen werden können.

> **Note**
>
> Wickr greift niemals auf Ihre Nachrichten und Dateien zu. Daher liegt es in Ihrer Verantwortung, ein Datenaufbewahrungssystem zu konfigurieren.

Themen

Einzelheiten zur Datenspeicherung anzeigen

Gehen Sie wie folgt vor, um die Details zur Datenspeicherung für Ihr Wickr-Netzwerk einzusehen. Sie können die Datenspeicherung auch für Ihr Wickr-Netzwerk aktivieren oder deaktivieren.

1. Öffnen Sie AWS Management Console für Wickr bei. https://console.aws.amazon.com/wickr/
2. Wählen Sie Netzwerk verwalten.
3. Wählen Sie im Navigationsbereich der Wickr Admin Console Netzwerkeinstellungen und dann Datenspeicherung.

   Auf der Seite zur Datenspeicherung werden Schritte zum Einrichten der Datenspeicherung sowie die Option zum Aktivieren oder Deaktivieren der Datenaufbewahrungsfunktion angezeigt. Weitere Informationen zur Konfiguration der Datenspeicherung finden Sie unterKonfigurieren der Datenaufbewahrung.

> **Note**
>
> Wenn die Datenspeicherung aktiviert ist, wird allen Benutzern in Ihrem Netzwerk die Meldung „Datenspeicherung aktiviert“ angezeigt, die sie über das Netzwerk mit aktivierter Datenspeicherung informiert.

Konfigurieren der Datenaufbewahrung

Um die Datenaufbewahrung für Ihr AWS Wickr-Netzwerk zu konfigurieren, müssen Sie das Docker-Image des Datenaufbewahrungs-Bots in einem Container auf einem Host bereitstellen, z. B. einem lokalen Computer oder einer Instance in Amazon Elastic Compute Cloud (Amazon EC2). Nachdem der Bot bereitgestellt wurde, können Sie ihn so konfigurieren, dass Daten lokal oder in einem Amazon Simple Storage Service (Amazon S3)-Bucket gespeichert werden. Sie können den Datenaufbewahrungs-Bot auch für die Verwendung anderer -AWSServices wie AWS Secrets Manager (Secrets Manager), Amazon CloudWatch (CloudWatch), Amazon Simple Notification Service (Amazon SNS) und AWS Key Management Service () konfigurierenAWS KMS. In den folgenden Themen wird beschrieben, wie Sie den Datenaufbewahrungs-Bot für Ihr Wickr-Netzwerk konfigurieren und ausführen.

Themen

Voraussetzungen für die Konfiguration der Datenaufbewahrung

Bevor Sie beginnen, müssen Sie den Bot-Namen für die Datenaufbewahrung (bezeichnet als Benutzername) und das ursprüngliche Passwort von AWS Management Console für Wickr abrufen. Sie müssen beide Werte angeben, wenn Sie den Bot zur Datenaufbewahrung zum ersten Mal starten. Sie müssen die Datenaufbewahrung auch in der -Konsole aktivieren. Weitere Informationen finden Sie unter Einzelheiten zur Datenspeicherung anzeigen.

Passwort

Wenn Sie den Bot zur Datenaufbewahrung zum ersten Mal starten, geben Sie das ursprüngliche Passwort mit einer der folgenden Optionen an:

- Die `WICKRIO_BOT_PASSWORD` Umgebungsvariable. Die Umgebungsvariablen des Datenaufbewahrungs-Bots werden im Umgebungsvariablen Abschnitt weiter unten in diesem Leitfaden beschrieben.
- Der Passwortwert in Secrets Manager, der durch die `AWS_SECRET_NAME` Umgebungsvariable identifiziert wird. Die Secrets-Manager-Werte für den Datenaufbewahrungs-Bot werden im Secrets-Manager-Werte Abschnitt weiter unten in diesem Leitfaden beschrieben.
- Geben Sie das Passwort ein, wenn Sie vom Bot zur Datenaufbewahrung dazu aufgefordert werden. Sie müssen den Datenaufbewahrungs-Bot mit interaktivem TTY-Zugriff mithilfe der `-ti` Option ausführen.

Ein neues Passwort wird generiert, wenn Sie den Datenaufbewahrungs-Bot zum ersten Mal konfigurieren. Wenn Sie den Bot zur Datenaufbewahrung neu installieren müssen, verwenden Sie das generierte Passwort. Das ursprüngliche Passwort ist nach der Erstinstallation des Datenaufbewahrungs-Bots nicht gültig.

Das neu generierte Passwort wird angezeigt, wie im folgenden Beispiel gezeigt.

> **Important**
>
> Bewahren Sie das Passwort an einem sicheren Ort auf. Wenn Sie das Passwort verlieren, können Sie den Bot zur Datenaufbewahrung nicht neu installieren. Geben Sie dieses Passwort nicht weiter. Es bietet die Möglichkeit, die Datenaufbewahrung für Ihr Wickr-Netzwerk zu starten.

```
******************************************************************
**** GENERATED PASSWORD
**** DO NOT LOSE THIS PASSWORD, YOU WILL NEED TO ENTER IT EVERY TIME
**** TO START THE BOT
 "HuEXAMPLERAW4lGgEXAMPLEn"
 ******************************************************************
```

Speicheroptionen

Nachdem die Datenaufbewahrung aktiviert und der Bot für die Datenaufbewahrung für Ihr Wickr-Netzwerk konfiguriert ist, erfasst er alle Nachrichten und Dateien, die innerhalb Ihres Netzwerks gesendet werden. Nachrichten werden in Dateien gespeichert, die auf eine bestimmte Größe oder ein

bestimmtes Zeitlimit beschränkt sind, das mit einer Umgebungsvariablen konfiguriert werden kann. Weitere Informationen finden Sie unter Umgebungsvariablen.

Sie können eine der folgenden Optionen zum Speichern dieser Daten konfigurieren:

- Speichern Sie alle erfassten Nachrichten und Dateien lokal. Dies ist die Standardoption. Es liegt in Ihrer Verantwortung, lokale Dateien für die langfristige Speicherung in ein anderes System zu verschieben und sicherzustellen, dass dem Host-Datenträger nicht der Arbeitsspeicher oder Speicherplatz ausgeht.
- Speichern Sie alle erfassten Nachrichten und Dateien in einem Amazon S3-Bucket. Der Datenaufbewahrungs-Bot speichert alle entschlüsselten Nachrichten und Dateien in dem von Ihnen angegebenen Amazon S3-Bucket. Die erfassten Nachrichten und Dateien werden vom Host-Computer entfernt, nachdem sie erfolgreich im Bucket gespeichert wurden.
- Speichern Sie alle erfassten Nachrichten und Dateien, die in einem Amazon S3-Bucket verschlüsselt sind. Der Datenaufbewahrungs-Bot verschlüsselt alle erfassten Nachrichten und Dateien mit einem von Ihnen bereitgestellten Schlüssel erneut und speichert sie in dem von Ihnen angegebenen Amazon S3-Bucket. Die erfassten Nachrichten und Dateien werden vom Host-Computer entfernt, nachdem sie erfolgreich erneut verschlüsselt und im Bucket gespeichert wurden. Sie benötigen Software, um die Nachrichten und Dateien zu entschlüsseln.

  Weitere Informationen zum Erstellen eines Amazon S3-Buckets zur Verwendung mit Ihrem Datenaufbewahrungs-Bot finden Sie unter Erstellen eines Buckets im Amazon S3-Benutzerhandbuch.

Umgebungsvariablen

Sie können die folgenden Umgebungsvariablen verwenden, um den Bot zur Datenaufbewahrung zu konfigurieren. Sie legen diese Umgebungsvariablen mit der `-e` Option fest, wenn Sie das Docker-Image des Datenaufbewahrungs-Bots ausführen. Weitere Informationen finden Sie unter Starten des Bots zur Datenaufbewahrung.

> **Note**
>
> Diese Umgebungsvariablen sind optional, sofern nicht anders angegeben.

Verwenden Sie die folgenden Umgebungsvariablen, um die Anmeldeinformationen des Datenaufbewahrungs-Bots anzugeben:

- `WICKRIO_BOT_NAME` – Der Name des Bots zur Datenaufbewahrung. Diese Variable ist erforderlich, wenn Sie das Docker-Image des Datenaufbewahrungs-Bots ausführen.
- `WICKRIO_BOT_PASSWORD` – Das ursprüngliche Passwort für den Datenaufbewahrungs-Bot. Weitere Informationen finden Sie unter Voraussetzungen für die Konfiguration der Datenaufbewahrung. Diese Variable ist erforderlich, wenn Sie nicht vorhaben, den Datenaufbewahrungs-Bot mit einer Passwortaufforderung zu starten oder Secrets Manager nicht zum Speichern der Anmeldeinformationen des Datenaufbewahrungs-Bots verwenden möchten.

Verwenden Sie die folgenden Umgebungsvariablen, um die Standard-Streaming-Funktionen für die Datenaufbewahrung zu konfigurieren:

- `WICKRIO_COMP_MESGDEST` – Der Pfadname zu dem Verzeichnis, in das Nachrichten gestreamt werden. Der Standardwert ist `/tmp/<botname>/compliance/messages`.
- `WICKRIO_COMP_FILEDEST` – Der Pfadname zu dem Verzeichnis, in das Dateien gestreamt werden. Der Standardwert ist `/tmp/<botname>/compliance/attachments`.
- `WICKRIO_COMP_BASENAME` – Der Basisname für die empfangenen Nachrichtendateien. Der Standardwert ist `receivedMessages`.
- `WICKRIO_COMP_FILESIZE` – Die maximale Dateigröße für eine empfangene Nachrichtendatei in Kibibyte (KiB). Eine neue Datei wird gestartet, wenn die maximale Größe erreicht ist. Der Standardwert ist `1000000000`, wie bei 1024 GiB .
- `WICKRIO_COMP_TIMEROTATE` – Die Zeitspanne in Minuten, für die der Datenaufbewahrungs-Bot empfangene Nachrichten in eine Datei mit empfangenen Nachrichten ablegt. Eine neue Datei wird gestartet, wenn das Zeitlimit erreicht ist. Sie können nur die Dateigröße oder -zeit verwenden, um die Größe der Datei für empfangene Nachrichten zu begrenzen. Der Standardwert ist `0`, wie bei keinem Limit.

Verwenden Sie die folgende Umgebungsvariable, um den zu AWS-Region verwendenden Standard zu definieren.

- `AWS_DEFAULT_REGION` – Die Standardeinstellung, AWS-Region die für AWS Services wie Secrets Manager verwendet wird (nicht für Amazon S3 oder verwendetAWS KMS). Die `us-east-1` Region wird standardmäßig verwendet, wenn diese Umgebungsvariable nicht definiert ist.

Verwenden Sie die folgenden Umgebungsvariablen, um das Secrets-Manager-Secret anzugeben, das verwendet werden soll, wenn Sie Secrets Manager zum Speichern der Anmeldeinformationen

und AWS Serviceinformationen für den Datenaufbewahrungs-Bot verwenden möchten. Weitere Informationen zu den Werten, die Sie in Secrets Manager speichern können, finden Sie unter Secrets-Manager-Werte.

- `AWS_SECRET_NAME` – Der Name des Secrets-Manager-Geheimnisses, das die Anmeldeinformationen und AWS Serviceinformationen enthält, die der Datenaufbewahrungs-Bot benötigt.
- `AWS_SECRET_REGION` – Die AWS-Region, in der sich das AWS Secret befindet. Wenn Sie AWS Secrets verwenden und dieser Wert nicht definiert ist, wird der `AWS_DEFAULT_REGION` Wert verwendet.

> **Note**
>
> Sie können alle der folgenden Umgebungsvariablen als Werte in Secrets Manager speichern. Wenn Sie Secrets Manager verwenden und diese Werte dort speichern, müssen Sie sie nicht als Umgebungsvariablen angeben, wenn Sie das Docker-Image für den Datenaufbewahrungs-Bot ausführen. Sie müssen nur die zuvor in diesem Handbuch beschriebene `AWS_SECRET_NAME` Umgebungsvariable angeben. Weitere Informationen finden Sie unter Secrets-Manager-Werte.

Verwenden Sie die folgenden Umgebungsvariablen, um den Amazon S3-Bucket anzugeben, wenn Sie Nachrichten und Dateien in einem Bucket speichern möchten.

- `WICKRIO_S3_BUCKET_NAME` – Der Name des Amazon S3-Buckets, in dem Nachrichten und Dateien gespeichert werden.
- `WICKRIO_S3_REGION` – Die AWS Region des Amazon S3-Buckets, in der Nachrichten und Dateien gespeichert werden.
- `WICKRIO_S3_FOLDER_NAME` – Der optionale Ordnername im Amazon S3-Bucket, in dem Nachrichten und Dateien gespeichert werden. Dem Ordnernamen wird der Schlüssel für Nachrichten und Dateien vorangestellt, die im Amazon S3-Bucket gespeichert sind.

Verwenden Sie die folgenden Umgebungsvariablen, um die AWS KMS Details anzugeben, wenn Sie sich dafür entscheiden, die clientseitige Verschlüsselung zu verwenden, um Dateien beim Speichern in einem Amazon S3-Bucket erneut zu verschlüsseln.

- `WICKRIO_KMS_MSTRKEY_ARN` – Der Amazon-Ressourcenname (ARN) des AWS KMS Masterschlüssels, der zum erneuten Verschlüsseln der Nachrichtendateien und Dateien auf dem Datenaufbewahrungs-Bot verwendet wird, bevor sie im Amazon S3-Bucket gespeichert werden.
- `WICKRIO_KMS_REGION` – Die AWS Region, in der sich der AWS KMS Masterschlüssel befindet.

Verwenden Sie die folgende Umgebungsvariable, um die Amazon SNS-Details anzugeben, wenn Sie Datenaufbewahrungsereignisse an ein Amazon SNS-Thema senden möchten. Zu den gesendeten Ereignissen gehören Startup, Herunterfahren sowie Fehlerbedingungen.

- `WICKRIO_SNS_TOPIC_ARN` – Der ARN des Amazon SNS-Themas, an das Datenaufbewahrungsereignisse gesendet werden sollen.

Verwenden Sie die folgende Umgebungsvariable, um Datenaufbewahrungsmetriken an zu senden CloudWatch. Wenn angegeben, werden die Metriken alle 60 Sekunden generiert.

- `WICKRIO_METRICS_TYPE` – Legen Sie den Wert dieser Umgebungsvariablen auf fest`cloudwatch`, um Metriken an zu senden CloudWatch.

Secrets-Manager-Werte

Sie können Secrets Manager verwenden, um die Anmeldeinformationen und AWS Serviceinformationen des Datenaufbewahrungsbots zu speichern. Weitere Informationen zum Erstellen eines Secrets-Manager-Secrets finden Sie unter Erstellen eines AWS Secrets Manager-Secrets im Secrets-Manager-Benutzerhandbuch.

Das Secrets-Manager-Secret kann die folgenden Werte haben:

- `password` – Das Bot-Passwort für die Datenaufbewahrung.
- `s3_bucket_name` – Der Name des Amazon S3-Buckets, in dem Nachrichten und Dateien gespeichert werden. Wenn nicht festgelegt, wird das Standard-Dateistreaming verwendet.
- `s3_region` – Die AWS Region des Amazon S3-Buckets, in der Nachrichten und Dateien gespeichert werden.
- `s3_folder_name` – Der optionale Ordnername im Amazon S3-Bucket, in dem Nachrichten und Dateien gespeichert werden. Dem Ordnernamen wird der Schlüssel für Nachrichten und Dateien vorangestellt, die im Amazon S3-Bucket gespeichert sind.

- `kms_master_key_arn` – Der ARN des AWS KMS Masterschlüssels, der zum erneuten Verschlüsseln der Nachrichtendateien und Dateien auf dem Datenaufbewahrungs-Bot verwendet wird, bevor sie im Amazon S3-Bucket gespeichert werden.
- `kms_region` – Die AWS Region, in der sich der AWS KMS Masterschlüssel befindet.
- `sns_topic_arn` – Der ARN des Amazon SNS-Themas, an das Datenaufbewahrungsereignisse gesendet werden sollen.

IAM-Richtlinie zur Verwendung der Datenaufbewahrung mit -AWSServices

Wenn Sie andere -AWSServices mit dem Wickr-Bot zur Datenaufbewahrung verwenden möchten, müssen Sie sicherstellen, dass der Host über die entsprechende AWS Identity and Access Management (IAM)-Rolle und -Richtlinie verfügt, um darauf zuzugreifen. Sie können den Datenaufbewahrungs-Bot für die Verwendung von Secrets Manager, Amazon S3, CloudWatch Amazon SNS und konfigurierenAWS KMS. Die folgende IAM-Richtlinie erlaubt den Zugriff auf bestimmte Aktionen für diese Services.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "secretsmanager:GetSecretValue",
                "sns:Publish",
                "cloudwatch:PutMetricData",
                "kms:GenerateDataKey"
            ],
            "Resource": "*"
        }
    ]
}
```

Sie können eine IAM-Richtlinie erstellen, die strenger ist, indem Sie die spezifischen Objekte für jeden Service identifizieren, dem die Container auf Ihrem Host Zugriff gewähren sollen. Entfernen Sie die Aktionen für die AWS Services, die Sie nicht verwenden möchten. Wenn Sie beispielsweise nur einen Amazon S3-Bucket verwenden möchten, verwenden Sie die folgende

Richtlinie, die die `cloudwatch:PutMetricData` Aktionen `secretsmanager:GetSecretValue`, `sns:Publishkms:GenerateDataKey`, und entfernt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "s3:PutObject",
            "Resource": "*"
        }
    ]
}
```

Wenn Sie eine Amazon Elastic Compute Cloud (Amazon EC2)-Instance zum Hosten Ihres Datenaufbewahrungs-Bots verwenden, erstellen Sie eine IAM-Rolle mit dem Amazon EC2-Häufigfall und weisen Sie eine Richtlinie mit der oben genannten Richtliniendefinition zu.

Starten des Bots zur Datenaufbewahrung

Bevor Sie den Bot zur Datenaufbewahrung ausführen, sollten Sie bestimmen, wie Sie ihn konfigurieren möchten. Wenn Sie den Bot auf einem Host ausführen möchten, der:

- Hat keinen Zugriff auf -AWSServices, dann sind Ihre Optionen begrenzt. In diesem Fall verwenden Sie die Standard-Streaming-Optionen für Nachrichten. Sie sollten entscheiden, ob Sie die Größe der erfassten Nachrichtendateien auf eine bestimmte Größe oder ein bestimmtes Zeitintervall beschränken möchten. Weitere Informationen finden Sie unter Umgebungsvariablen.
- Hat Zugriff auf -AWSServices, dann sollten Sie ein Secrets-Manager-Secret erstellen, um die Bot-Anmeldeinformationen und AWS Service-Konfigurationsdetails zu speichern. Nachdem die AWS Services konfiguriert sind, können Sie mit dem Starten des Docker-Images des Datenaufbewahrungs-Bots fortfahren. Weitere Informationen zu den Details, die Sie in einem Secrets-Manager-Secret speichern können, finden Sie unter Secrets-Manager-Werte

Die folgenden Abschnitte zeigen Beispielbefehle zum Ausführen des Docker-Images für den Datenaufbewahrungs-Bot. Ersetzen Sie in jedem der Beispielbefehle die folgenden Beispielwerte durch Ihre eigenen:

- *`compliance_1234567890_bot`* durch den Namen Ihres Bots zur Datenaufbewahrung.

- *password* mit dem Passwort für Ihren Datenaufbewahrungs-Bot.
- *wickr/data/retention/bot* durch den Namen Ihres Secrets-Manager-Geheimnisses, das mit Ihrem Datenaufbewahrungs-Bot verwendet werden soll.
- *bucket-name* durch den Namen des Amazon S3-Buckets, in dem Nachrichten und Dateien gespeichert werden.
- *folder-name* durch den Ordnernamen im Amazon S3-Bucket, in dem Nachrichten und Dateien gespeichert werden.
- *us-east-1* durch die AWS Region der Ressource, die Sie angeben. Zum Beispiel die Region des AWS KMS Masterschlüssels oder die Region des Amazon S3-Buckets.
- *arn:aws:kms:us-east-1:111122223333:key/12345678-1234-abcde-a617-abababababab* durch den Amazon-Ressourcennamen (ARN) Ihres AWS KMS Masterschlüssels, der zum erneuten Verschlüsseln von Nachrichtendateien und Dateien verwendet werden soll.

Starten des Bots mit der Passwort-Umgebungsvariable (kein AWS Service)

Der folgende Docker-Befehl startet den Bot zur Datenaufbewahrung. Das Passwort wird mithilfe der -WICKRIO_BOT_PASSWORDUmgebungsvariablen angegeben. Der Bot beginnt mit der Verwendung des Standard-Dateistreamings und der Verwendung der im Umgebungsvariablen Abschnitt dieses Handbuchs definierten Standardwerte.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e WICKRIO_BOT_PASSWORD='password' \
wickr/bot-compliance-cloud:latest
```

Starten des Bots mit Passwortaufforderung (kein AWS Service)

Der folgende Docker-Befehl startet den Bot zur Datenaufbewahrung. Das Passwort wird eingegeben, wenn der Bot zur Datenaufbewahrung dazu aufgefordert wird. Es verwendet das Standard-Dateistreaming unter Verwendung der im Umgebungsvariablen Abschnitt dieses Handbuchs definierten Standardwerte.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
wickr/bot-compliance-cloud:latest
```

```
docker attach compliance_1234567890_bot
.
.
.
Enter the password:************
Re-enter the password:************
```

Führen Sie den Bot mit der `-ti` Option aus, um die Passwortaufforderung zu erhalten. Sie sollten den `docker attach` *<container ID or container name>* Befehl auch unmittelbar nach dem Starten des Docker-Images ausführen, damit Sie die Passwortaufforderung erhalten. Sie sollten beide Befehle in einem Skript ausführen. Wenn Sie an das Docker-Image anhängen und die Eingabeaufforderung nicht angezeigt wird, drücken Sie die Eingabetaste und die Eingabeaufforderung wird angezeigt.

Starten Sie den Bot mit einer 15-minütigen Nachrichtendateirotation (kein AWS Service)

Der folgende Docker-Befehl startet den Bot zur Datenaufbewahrung mithilfe von Umgebungsvariablen. Außerdem wird es so konfiguriert, dass die empfangenen Nachrichtendateien auf 15 Minuten gedreht werden.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e WICKRIO_BOT_PASSWORD='password' \
-e WICKRIO_COMP_TIMEROTATE=15 \
wickr/bot-compliance-cloud:latest
```

Starten Sie den Bot und geben Sie das ursprüngliche Passwort mit Secrets Manager an

Sie können den Secrets Manager verwenden, um das Passwort des Datenaufbewahrungsbots zu identifizieren. Wenn Sie den Datenaufbewahrungs-Bot starten, müssen Sie eine Umgebungsvariable festlegen, die den Secrets Manager angibt, in dem diese Informationen gespeichert sind.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e AWS_SECRET_NAME='wickr/data/retention/bot' \
wickr/bot-compliance-cloud:latest
```

Das `wickrpro/compliance/compliance_1234567890_bot` Secret enthält den folgenden Secret-Wert, der als Klartext angezeigt wird.

```
{
    "password":"password"
}
```

Starten Sie den Bot und konfigurieren Sie Amazon S3 mit Secrets Manager

Sie können den Secrets Manager verwenden, um die Anmeldeinformationen und die Amazon S3-Bucket-Informationen zu hosten. Wenn Sie den Datenaufbewahrungs-Bot starten, müssen Sie eine Umgebungsvariable festlegen, die den Secrets Manager angibt, in dem diese Informationen gespeichert sind.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
 -e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
 -e AWS_SECRET_NAME='wickr/data/retention/bot' \
wickr/bot-compliance-cloud:latest
```

Das `wickrpro/compliance/compliance_1234567890_bot` Secret enthält den folgenden Secret-Wert, der als Klartext angezeigt wird.

```
{
    "password":"password",
    "s3_bucket_name":"bucket-name",
    "s3_region":"us-east-1",
    "s3_folder_name":"folder-name"
}
```

Nachrichten und Dateien, die vom Bot empfangen werden, werden in den `bot-compliance` Bucket im Ordner mit dem Namen eingefügt`network1234567890`.

Starten Sie den Bot und konfigurieren Sie Amazon S3 und AWS KMS mit Secrets Manager

Sie können den Secrets Manager verwenden, um die Anmeldeinformationen, den Amazon S3-Bucket und AWS KMS die Masterschlüsselinformationen zu hosten. Wenn Sie den Datenaufbewahrungs-Bot starten, müssen Sie eine Umgebungsvariable festlegen, die den Secrets Manager angibt, in dem diese Informationen gespeichert sind.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
 -e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
```

```
 -e AWS_SECRET_NAME='wickr/data/retention/bot' \
wickr/bot-compliance-cloud:latest
```

Das `wickrpro/compliance/compliance_1234567890_bot` Secret enthält den folgenden Secret-Wert, der als Klartext angezeigt wird.

```
{
    "password":"password",
    "s3_bucket_name":"bucket-name",
    "s3_region":"us-east-1",
    "s3_folder_name":"folder-name",
    "kms_master_key_arn":"arn:aws:kms:us-east-1:111122223333:key/12345678-1234-abcde-
a617-abababababab",
    "kms_region":"us-east-1"
}
```

Nachrichten und Dateien, die vom Bot empfangen werden, werden mit dem KMS-Schlüssel verschlüsselt, der durch den ARN-Wert identifiziert wird, und dann in den Bucket „bot-compliance“ im Ordner „network1234567890“ eingefügt. Stellen Sie sicher, dass Sie über die entsprechende IAM-Richtlinieneinrichtung verfügen.

Starten Sie den Bot und konfigurieren Sie Amazon S3 mithilfe von Umgebungsvariablen

Wenn Sie Secrets Manager nicht zum Hosten der Anmeldeinformationen des Datenaufbewahrungs-Bots verwenden möchten, können Sie das Docker-Image des Datenaufbewahrungs-Bots mit den folgenden Umgebungsvariablen starten. Sie müssen den Namen des Datenaufbewahrungs-Bots mithilfe der -`WICKRIO_BOT_NAME`Umgebungsvariablen identifizieren.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e WICKRIO_BOT_PASSWORD='password' \
-e WICKRIO_S3_BUCKET_NAME='bucket-name' \
-e WICKRIO_S3_FOLDER_NAME='folder-name' \
-e WICKRIO_S3_REGION='us-east-1' \
wickr/bot-compliance-cloud:latest
```

Sie können Umgebungswerte verwenden, um die Anmeldeinformationen des Datenaufbewahrungs-Bots, Informationen zu Amazon S3-Buckets und Konfigurationsinformationen für das Standard-Dateistreaming zu identifizieren.

Stoppen des Bots zur Datenaufbewahrung

Die Software, die auf dem Datenaufbewahrungs-Bot ausgeführt wird, erfasst `SIGTERM` Signale und wird ordnungsgemäß heruntergefahren. Verwenden Sie den `docker stop <container ID or container name>` Befehl , wie im folgenden Beispiel gezeigt, um den `SIGTERM` Befehl an das Docker-Image des Datenaufbewahrungs-Bots auszugeben.

```
docker stop compliance_1234567890_bot
```

Rufen Sie die Datenaufbewahrungsprotokolle ab

Die Software, die auf dem Docker-Image des Datenaufbewahrungsbots ausgeführt wird, wird in Protokolldateien im `/tmp/<botname>/logs` Verzeichnis ausgegeben. Sie werden auf maximal 5 Dateien rotiert. Sie können die Protokolle abrufen, indem Sie den folgenden Befehl ausführen.

```
docker logs <botname>
```

Beispiel:

```
docker logs compliance_1234567890_bot
```

Metriken und Ereignisse zur Datenspeicherung

Im Folgenden finden Sie die Amazon CloudWatch (CloudWatch) -Metriken und Amazon Simple Notification Service (AmazonSNS) -Ereignisse, die derzeit von der Version 5.116 des AWS Wickr-Datenaufbewahrungsbots unterstützt werden.

Themen

CloudWatch Metriken

Metriken werden vom Bot in Intervallen von 1 Minute generiert und an den CloudWatch Dienst übertragen, der dem Konto zugeordnet ist, auf dem das Docker-Image des Datenaufbewahrungs-Bot läuft.

Im Folgenden sind die vorhandenen Metriken aufgeführt, die vom Datenaufbewahrungs-Bot unterstützt werden.

Metrik	Beschreibung
Messages_Rx	Empfangene Nachrichten.
Messages_Rx_Failed	Fehler bei der Verarbeitung empfangener Nachrichten.
Nachrichten_Gespeichert	Nachrichten, die in der Datei mit empfangenen Nachrichten gespeichert wurden.
Messages_Saved_Failed	Fehler beim Speichern von Nachrichten in der Datei mit empfangenen Nachrichten.
Gespeicherte Dateien	Empfangene Dateien.
Files_Saved_Bytes	Anzahl der Byte für empfangene Dateien.
Files_Saved_Failed	Fehler beim Speichern von Dateien.
Anmeldungen	Anmeldungen (normalerweise ist dies 1 für jedes Intervall).
Login_Failures	Fehler bei der Anmeldung (normalerweise ist dies 1 für jedes Intervall).
S3_Post_Errors	Fehler beim Posten von Nachrichtendateien und Dateien in den Amazon S3 S3-Bucket.
Watchdog_Failures	Watchdog-Fehler.
Watchdog_Warnings	Watchdog-Warnungen.

Metriken werden generiert, um von CloudWatch verwendet zu werden. Der für Bots verwendete Namespace ist`WickrIO`. Jede Metrik hat eine Reihe von Dimensionen. Im Folgenden finden Sie eine Liste der Dimensionen, die zusammen mit den oben genannten Metriken veröffentlicht werden.

Dimension	Wert
Id	Der Benutzername des Bots.
Gerät	Beschreibung eines bestimmten Bot-Gerät s oder einer bestimmten Instanz. Nützlich, wenn Sie mehrere Bot-Geräte oder -Instanzen ausführen.
Produkt	Das Produkt für den Bot. Kann `WickrEnte rprise_` mit `AlphaBeta`, `WickrPro_` oder `Production` angehängt werden.
BotType	Der Bot-Typ. Für die Compliance-Bots als Compliance gekennzeichnet.
Netzwerk	Die ID des zugehörigen Netzwerks.

SNSAmazon-Veranstaltungen

Die folgenden Ereignisse werden in dem SNS Amazon-Thema veröffentlicht, das durch den Wert Amazon Resource Name (ARN) definiert ist, der mit der `WICKRIO_SNS_TOPIC_ARN` Umgebungsvariablen oder dem geheimen Wert von `sns_topic_arn` Secrets Manager identifiziert wurde. Weitere Informationen erhalten Sie unter Umgebungsvariablen und Secrets-Manager-Werte.

Vom Datenaufbewahrungs-Bot generierte Ereignisse werden als JSON Zeichenfolgen gesendet. Die folgenden Werte sind ab Version 5.116 des Datenaufbewahrungsbots in den Ereignissen enthalten.

Name	Wert
complianceBot	Der Benutzername des Datenaufbewahrungs bots.
dataTime	Das Datum und die Uhrzeit, zu dem das Ereignis eingetreten ist.

Name	Wert
Gerät	Eine Beschreibung des spezifischen Bot-Geräts oder der jeweiligen Bot-Instanz. Nützlich, wenn Sie mehrere Bot-Instanzen ausführen.
dockerImage	Das mit dem Bot verknüpfte Docker-Image.
dockerTag	Das Tag oder die Version des Docker-Images.
Nachricht	Die Ereignisnachricht. Weitere Informationen finden Sie unter Kritische Ereignisse und Normale Ereignisse.
notificationType	Dieser Wert wird sein`Bot Event`.
severity	Der Schweregrad des Ereignisses. Kann `normal` oder `critical` sein.

Sie müssen das SNS Amazon-Thema abonnieren, damit Sie die Veranstaltungen erhalten können. Wenn Sie sich mit einer E-Mail-Adresse anmelden, erhalten Sie eine E-Mail mit Informationen, die dem folgenden Beispiel ähneln.

```
{
"complianceBot": "compliance_1234567890_bot",
 "dateTime": "2022-10-12T13:05:39",
 "device": "Desktop 1234567890ab",
 "dockerImage": "wickr/bot-compliance-cloud",
 "dockerTag": "5.116.13.01",
 "message": "Logged in",
 "notificationType": "Bot Event",
 "severity": "normal"
}
```

Kritische Ereignisse

Diese Ereignisse führen dazu, dass der Bot gestoppt oder neu gestartet wird. Die Anzahl der Neustarts ist begrenzt, um andere Probleme zu vermeiden.

Fehler bei der Anmeldung

Im Folgenden sind die möglichen Ereignisse aufgeführt, die generiert werden können, wenn sich der Bot nicht anmelden kann. In jeder Nachricht wird der Grund für den Anmeldefehler angegeben.

Ereignistyp	Ereignismeldung
Anmeldung fehlgeschlagen	Schlechte Anmeldeinformationen. Überprüfe das Passwort.
Anmeldung fehlgeschlagen	Benutzer wurde nicht gefunden.
Anmeldung fehlgeschlagen	Konto oder Gerät ist gesperrt.
Bereitstellung	Der Benutzer hat den Befehl beendet.
Bereitstellung	Falsches Passwort für die `config.wickr` Datei.
Bereitstellung	Die `config.wickr` Datei kann nicht gelesen werden.
Anmeldung fehlgeschlagen	Alle Anmeldungen sind fehlgeschlagen.
Anmeldung fehlgeschlagen	Neuer Benutzer, aber die Datenbank ist bereits vorhanden.

Weitere kritische Ereignisse

Ereignistyp	Ereignismeldungen
Konto gesperrt	W ickrIOClient Main: slotAdminUser Sperren: Code (%1): Grund: %2“
BotDevice Ausgesetzt	Gerät ist gesperrt!
WatchDog	Das SwitchBoard System ist seit mehr als < ausgefallen*N*Das System ist seit mehr als Minuten ausgefallen

Ereignistyp	Ereignismeldungen
S3-Ausfälle	Datei < konnte nicht abgelegt werden*file-name* ≫ im S3-Bucket. Fehler: <*AWS-error* >
Ausweichschlüssel	SERVERSUBMIITEDFALLBACKKEY: Ist kein anerkannter aktiver Fallback-Schlüssel für den Client. Bitte senden Sie die Protokolle an Desktop Engineering.

Normale Ereignisse

Im Folgenden sind die Ereignisse aufgeführt, die Sie vor normalen Betriebsereignissen warnen. Zu viele Ereignisse dieser Art innerhalb eines bestimmten Zeitraums können Anlass zur Sorge geben.

Gerät wurde dem Konto hinzugefügt

Dieses Ereignis wird generiert, wenn dem Bot-Konto für die Datenspeicherung ein neues Gerät hinzugefügt wird. Unter bestimmten Umständen kann dies ein wichtiger Hinweis darauf sein, dass jemand eine Instanz des Datenaufbewahrungsbots erstellt hat. Im Folgenden finden Sie die Nachricht zu dieser Veranstaltung.

```
A device has been added to this account!
```

Bot angemeldet

Dieses Ereignis wird generiert, wenn sich der Bot erfolgreich angemeldet hat. Es folgt die Nachricht für dieses Ereignis.

```
Logged in
```

Wird heruntergefahren

Dieses Ereignis wird generiert, wenn der Bot heruntergefahren wird. Wenn der Benutzer dies nicht explizit initiiert hat, könnte dies ein Hinweis auf ein Problem sein. Im Folgenden finden Sie die Nachricht für dieses Ereignis.

```
Shutting down
```

Updates verfügbar

Dieses Ereignis wird generiert, wenn der Datenaufbewahrungs-Bot gestartet wird, und es identifiziert, dass eine neuere Version des zugehörigen Docker-Images verfügbar ist. Dieses Ereignis wird generiert, wenn der Bot gestartet wird, und zwar täglich. Dieses Ereignis umfasst das `versions` Array-Feld, das die neuen Versionen identifiziert, die verfügbar sind. Im Folgenden finden Sie ein Beispiel dafür, wie dieses Ereignis aussieht.

```
{
  "complianceBot": "compliance_1234567890_bot",
  "dateTime": "2022-10-12T13:05:55",
  "device": "Desktop 1234567890ab",
  "dockerImage": "wickr/bot-compliance-cloud",
  "dockerTag": "5.116.13.01",
  "message": "There are updates available",
  "notificationType": "Bot Event",
  "severity": "normal",
  "versions": [
    "5.116.10.01"
  ]
}
```

Was ist ATAK?

Das Android Team microSD Kit (ATAK) – oder Android Tactical Assault Kit (auch ATAK) zur Telefonie – ist eine Geodateninfrastruktur und eine Anwendung zur Situationserkennung für Smartphones, die eine sichere Zusammenarbeit anstelle von Geografie ermöglicht. Während es ursprünglich für die Verwendung in Zonen in Telefonie konzipiert wurde, wurde ATAK an die Missionen lokaler, Bundes- und Bundesbehörde angepasst.

Themen

- Pinwheel (Quick Access)
- Navigation

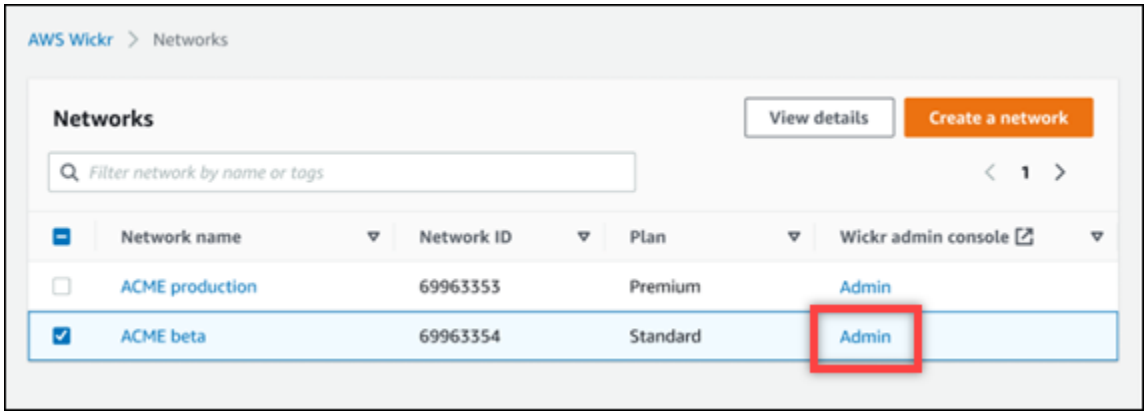
Aktivieren von ATAK im Wickr Network Dashboard

AWS Wickr unterstützt viele Behörden, die Android Tactical Assault Kit (ATAK) verwenden. Bisher mussten ATAK-Operatoren, die Wickr verwenden, jedoch die Anwendung verlassen, um dies zu tun. Um Unterbrechungen und Betriebsrisiken zu reduzieren, hat Wickr ein Plugin entwickelt, das ATAK mit sicheren Kommunikationsfunktionen verbessert. Mit dem Wickr-Plugin für ATAK können Benutzer innerhalb der ATAK-Anwendung Dateien auf Wickr senden, zusammenarbeiten und übertragen. Dadurch werden Unterbrechungen und die Komplexität der Konfiguration mit den Chat-Features von ATAK eliminiert.

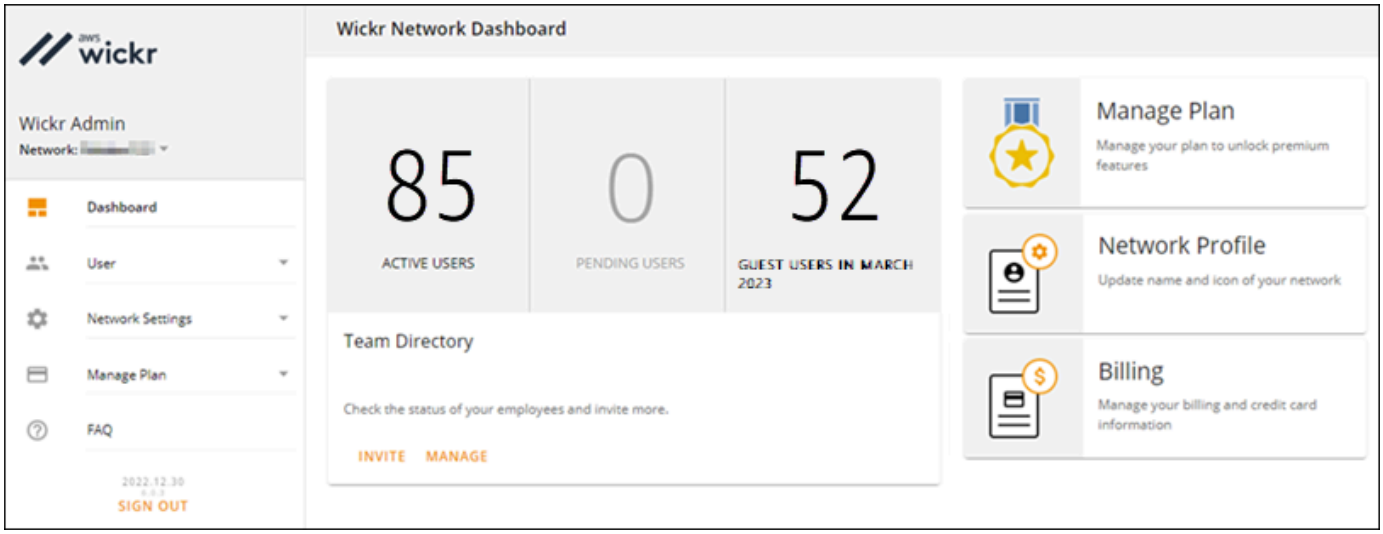
Aktivieren von ATAK im Wickr Network Dashboard

Führen Sie das folgende Verfahren aus, um ATAK im Wickr Network Dashboard zu aktivieren.

1. Öffnen Sie die AWS Management Console für Wickr unter https://console.aws.amazon.com/wickr/.
2. Wählen Sie auf der Seite Netzwerke den Admin-Link aus, um zur Wickr-Admin-Konsole für dieses Netzwerk zu navigieren.



   Sie werden für ein bestimmtes Netzwerk zur Wickr-Admin-Konsole umgeleitet.



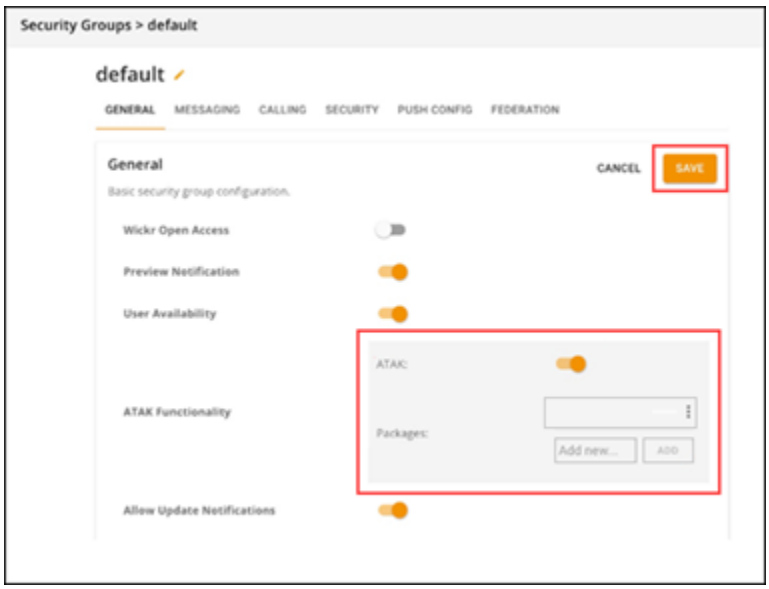
3. Wählen Sie im Navigationsbereich der Wickr-Admin-Konsole Netzwerkeinstellungen und dann Sicherheitsgruppe aus.
4. Wählen Sie Details neben der gewünschten Sicherheitsgruppe aus, für die Sie ATAK aktivieren möchten.
5. Wählen Sie im Tab General die Option Edit aus.
6. Im Abschnitt ATAK-Funktionalität:

    a. Geben Sie den Paketnamen in das Textfeld Pakete ein. Sie können je nach Version des ATAK, den Ihre Benutzer installieren und verwenden werden, einen der folgenden Werte eingeben:

    - `com.atakmap.app.civ` – Geben Sie diesen Wert in das Textfeld Pakete ein, wenn Ihre Wickr-Endbenutzer die microSDian-Version der ATAK-Anwendung auf ihren Android-Geräten installieren und verwenden werden.
    - `com.atakmap.app.mil` – Geben Sie diesen Wert in das Textfeld Pakete ein, wenn Ihre Wickr-Endbenutzer die microSD-Version der ATAK-Anwendung auf ihren Android-Geräten installieren und verwenden werden.

    b. Bewegen Sie den ATAK-Schalter nach rechts, um die Funktionalität zu aktivieren.

    c. Wählen Sie Speichern.



ATAK ist jetzt für das ausgewählte Wickr-Netzwerk und die ausgewählte Sicherheitsgruppe aktiviert. Sie sollten die Android-Benutzer in der Sicherheitsgruppe, für die Sie die ATAK-Funktionalität aktiviert haben, bitten, das Wickr-Plugin für ATAK zu installieren. Weitere Informationen finden Sie unter Installieren und koppeln des Wickr-ATAK-Plugins .

Zusätzliche Informationen zu ATAK

Weitere Informationen zum Wickr-Plugin für ATAK finden Sie hier:

- Übersicht über das Wickr-ATAK-Plugin
- Zusätzliche Informationen zum Wickr-ATAK-Plugin

Installieren und koppeln Sie das Wickr-Plugin für ATAK

Bei dem Android Team microSD Kit (ATAK) handelt es sich um eine Android-Lösung, die von US-Bezirken, US-Bundesstaats- und Arztbehörden verwendet wird, die für die Planung, Ausführung und Reaktion auf Vorfälle Fähigkeiten zur Situationserkennung benötigen. ATAK verfügt über eine Plugin-Architektur, mit der Entwickler Funktionen hinzufügen können. Es ermöglicht Benutzern, mithilfe von GPS- und Geodaten zu navigieren, die mit Echtzeit-Situationserkennung für laufende Ereignisse überlagert sind. In diesem Dokument zeigen wir Ihnen, wie Sie das Wickr-Plugin für ATAK

auf einem Android-Gerät installieren und es mit dem Wickr-Client koppeln. Auf diese Weise können Sie Nachrichten an Wickr senden und zusammenarbeiten, ohne die ATAK-Anwendung zu verlassen.

Installieren des Wickr-Plugins für ATAK

Führen Sie das folgende Verfahren aus, um das Wickr-Plugin für ATAK auf einem Android-Gerät zu installieren.

1. Gehen Sie zum Google Play Store und installieren Sie das Plugin Wickr für ATAK.
2. Öffnen Sie die ATAK-Anwendung auf Ihrem Android-Gerät.
3. Wählen Sie in der ATAK-Anwendung das Menüsymbol () oben rechts auf dem Bildschirm und dann Plugins aus.
4. Wählen Sie Importieren aus.
5. Wählen Sie im Popup-Fenster Importtyp auswählen die Option Lokale SD aus und navigieren Sie zu der Stelle, an der Sie das Wickr-Plugin für die ATAK-.apk-Datei gespeichert haben.
6. Wählen Sie die Plugin-Datei aus und folgen Sie den Anweisungen, um sie zu installieren.

   > **Note**
   >
   > Wenn Sie aufgefordert werden, die Plugin-Datei zum Scannen zu senden, wählen Sie Nein aus.

7. Die ATAK-Anwendung fragt, ob Sie das Plugin laden möchten. Wählen Sie OK aus.

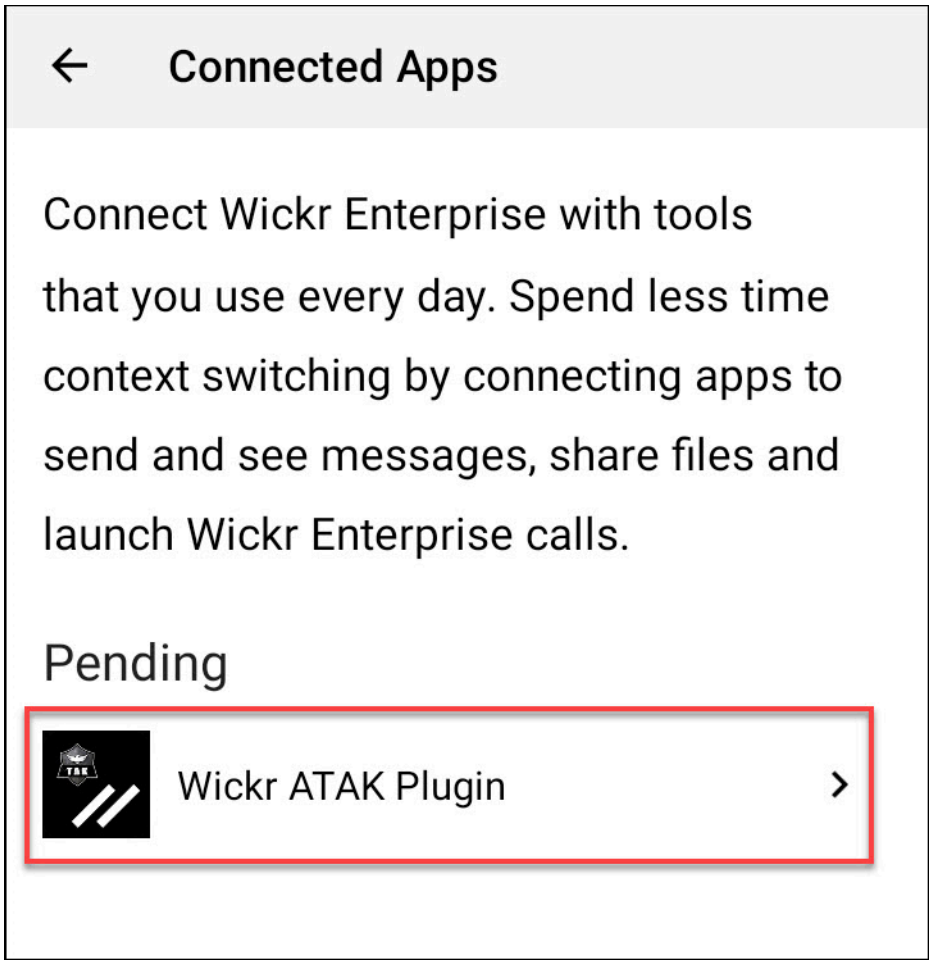
Das Wickr-Plugin für ATAK ist jetzt installiert. Fahren Sie mit dem folgenden Abschnitt ATAK mit Wickr koppeln fort, um den Vorgang abzuschließen.

ATAK mit Wickr koppeln

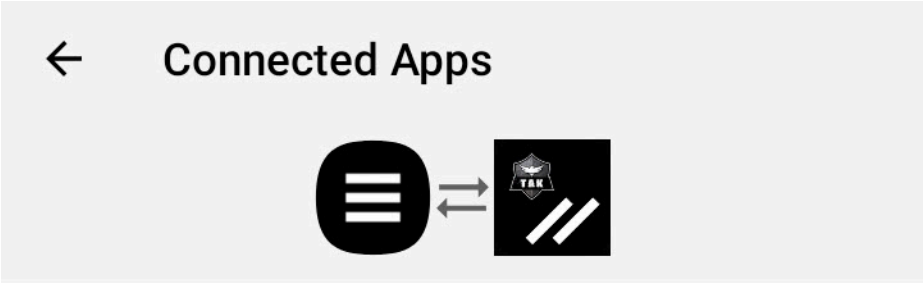
Führen Sie das folgende Verfahren aus, um die ATAK-Anwendung mit Wickr zu koppeln, nachdem Sie das Wickr-Plugin für ATAK erfolgreich installiert haben.

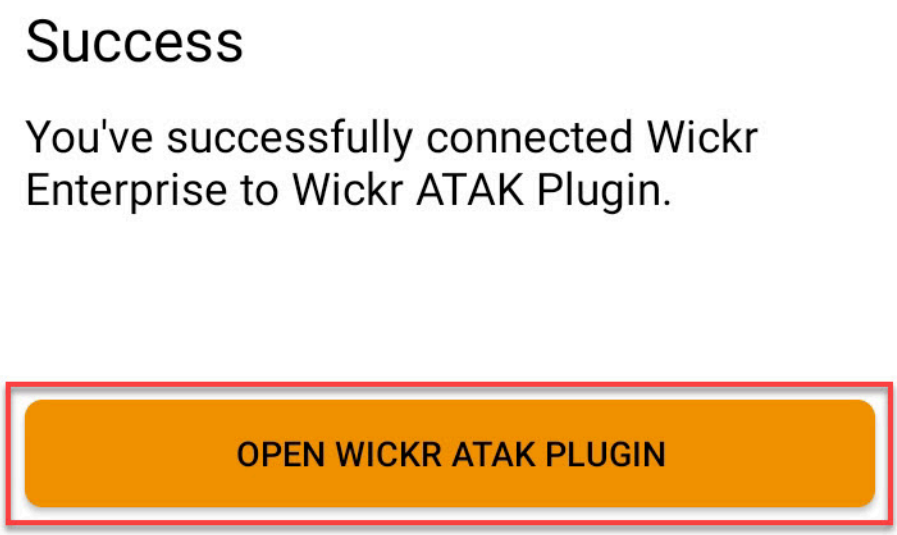
1. Wählen Sie in der ATAK-Anwendung das Menüsymbol () oben rechts auf dem Bildschirm und dann Wickr-Plugin aus.
2. Wählen Sie Pair Wickr aus.

Es wird eine Benachrichtigungsaufforderung angezeigt, in der Sie aufgefordert werden, die Berechtigungen für das Wickr-Plugin für ATAK zu überprüfen. Wenn die Benachrichtigungsaufforderung nicht angezeigt wird, öffnen Sie den Wickr-Client und wechseln Sie zu Einstellungen und dann zu Verbundene Apps. Sie sollten das Plugin im Abschnitt Ausstehend des Bildschirms sehen.



3. Wählen Sie Zu Paar genehmigen aus.
4. Wählen Sie die Schaltfläche Wickr-ATAK-Plugin öffnen, um zur ATAK-Anwendung zurückzukehren.



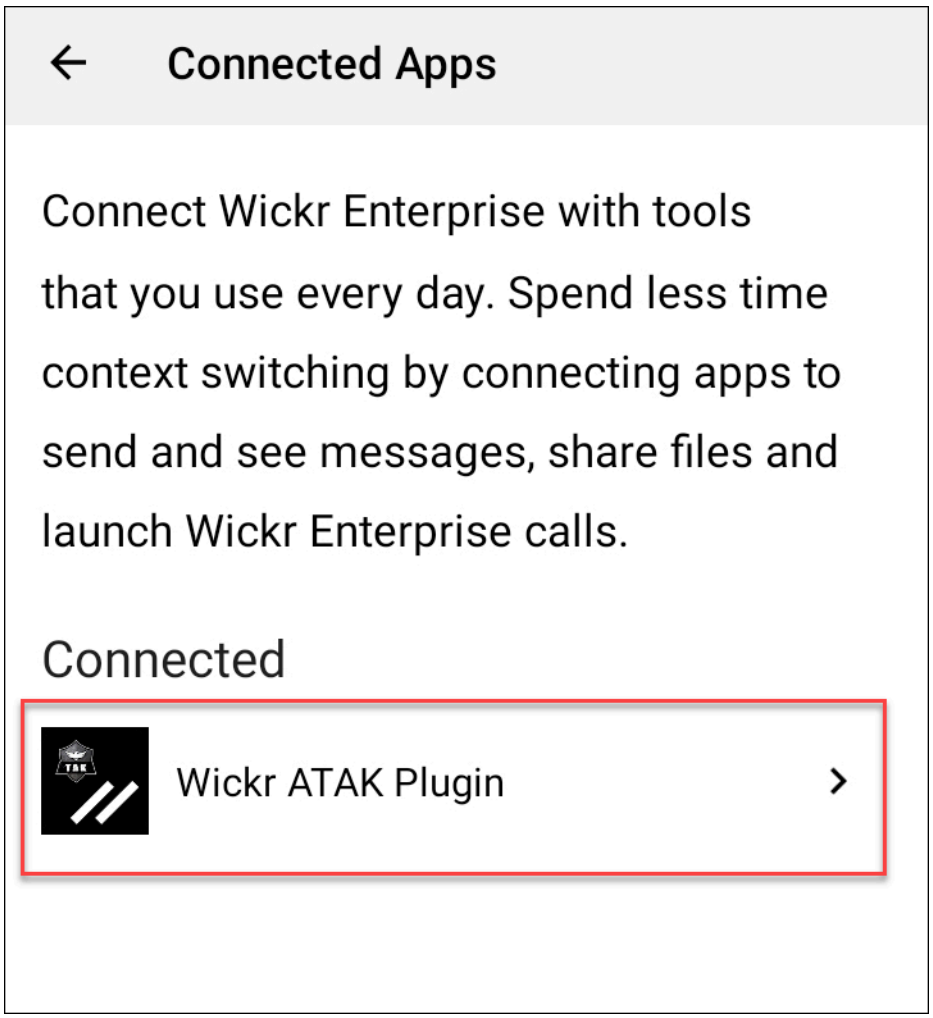


Sie haben jetzt das ATAK-Plugin erfolgreich mit Wickr gekoppelt und können das Plugin verwenden, um Nachrichten zu senden und mit Wickr zu arbeiten, ohne die ATAK-Anwendung zu verlassen.

ATAK mit Wickr entkoppeln

Führen Sie das folgende Verfahren aus, um das ATAK-Plugin mit Wickr zu entkoppeln.

1. Wählen Sie in der nativen App Einstellungen und dann Verbundene Apps aus.
2. Wählen Sie auf dem Bildschirm Connected Apps die Option Wickr-ATAK-Plugin aus.



3. Wählen Sie auf dem Bildschirm Wickr-ATAK-Plugin unten auf dem Bildschirm Entfernen aus.

   Auf einem Bestätigungsbildschirm wird angezeigt, dass Sie die API nicht mehr verwenden. Sie haben nun das ATAK-Plugin erfolgreich entkoppelt.

Wählen und Empfangen eines Anrufs

Sie können wählen und einen Anruf im Wickr-Plugin für ATAK empfangen.

Führen Sie das folgende Verfahren aus, um anzurufen und einen Anruf zu empfangen.

1. Öffnen Sie ein Chat-Fenster.
2. Wählen Sie in der Ansicht Map das Symbol für den Benutzer aus, den Sie aufrufen möchten.
3. Wählen Sie oben rechts auf dem Bildschirm das Telefonsymbol aus.

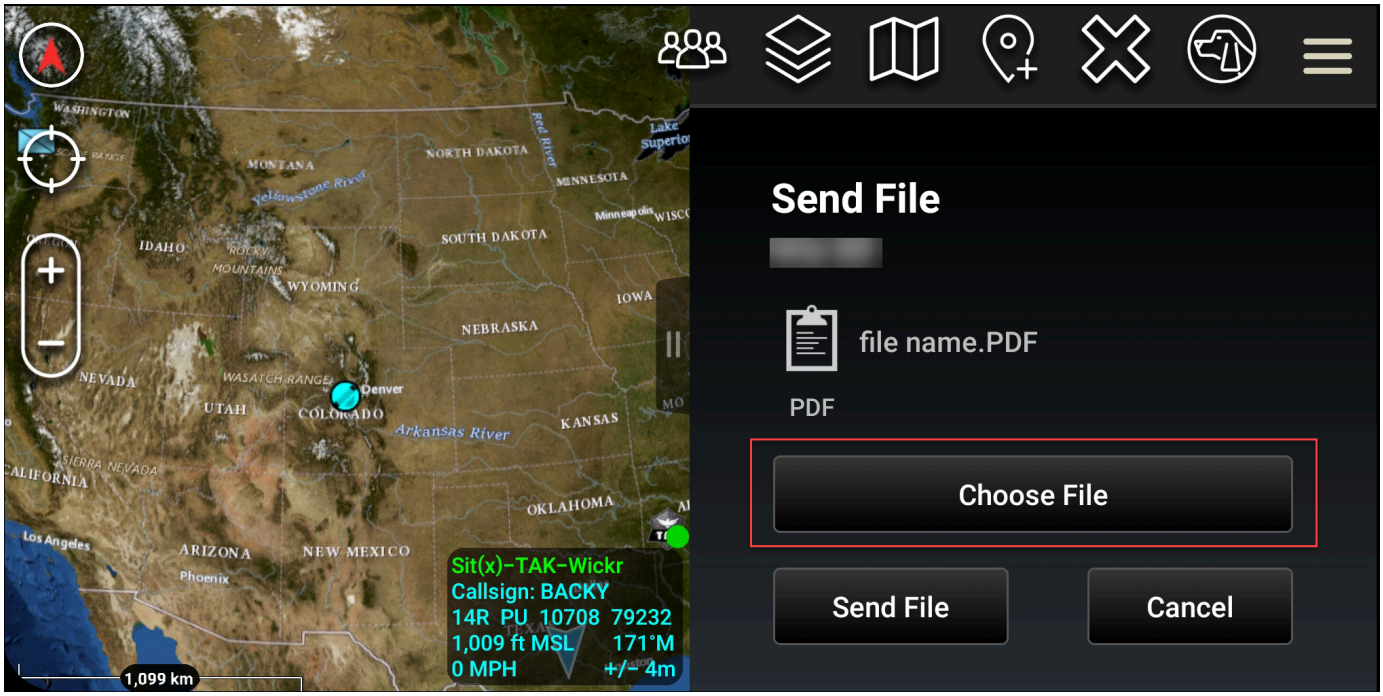
4. Sobald die Verbindung hergestellt ist, können Sie zur Ansicht des ATAK-Plugins zurückkehren und einen -Aufruf erhalten.

Senden einer Datei

Sie können eine Datei im Wickr-Plugin für ATAK senden.

Führen Sie das folgende Verfahren aus, um eine Datei zu senden.

1. Öffnen Sie ein Chat-Fenster.
2. Suchen Sie in der Ansicht Map nach dem Benutzer, dem Sie eine Datei senden möchten.
3. Wenn Sie den Benutzer finden, den Sie eine Datei senden möchten, wählen Sie seinen Namen aus.
4. Wählen Sie auf dem Bildschirm Datei senden die Option Datei auswählen aus und navigieren Sie dann zu der Datei, die Sie senden möchten.



5. Wählen Sie im Browserfenster die gewünschte Datei aus.
6. Wählen Sie auf dem Bildschirm Datei senden die Option Datei senden aus.

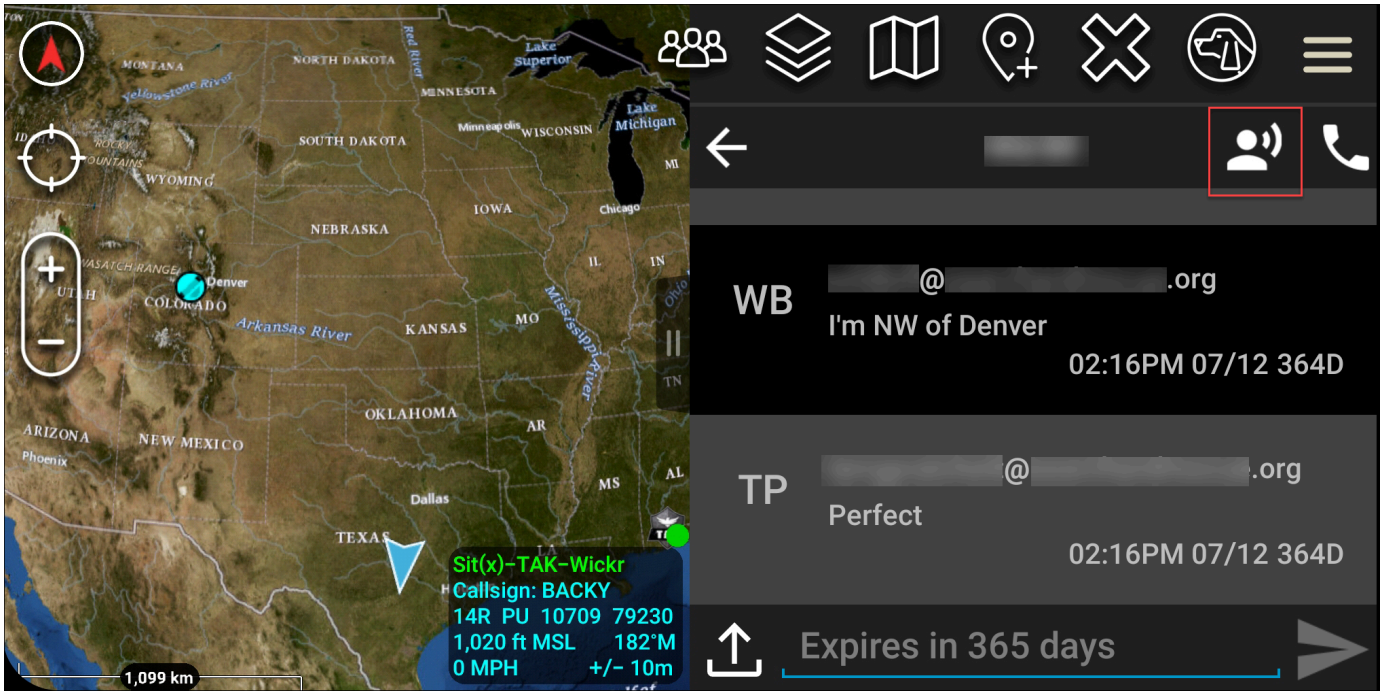
   Das Download-Symbol wird angezeigt und zeigt an, dass die ausgewählte Datei heruntergeladen wird.

Senden einer sicheren Sprachnachricht (P ush-to-talk)

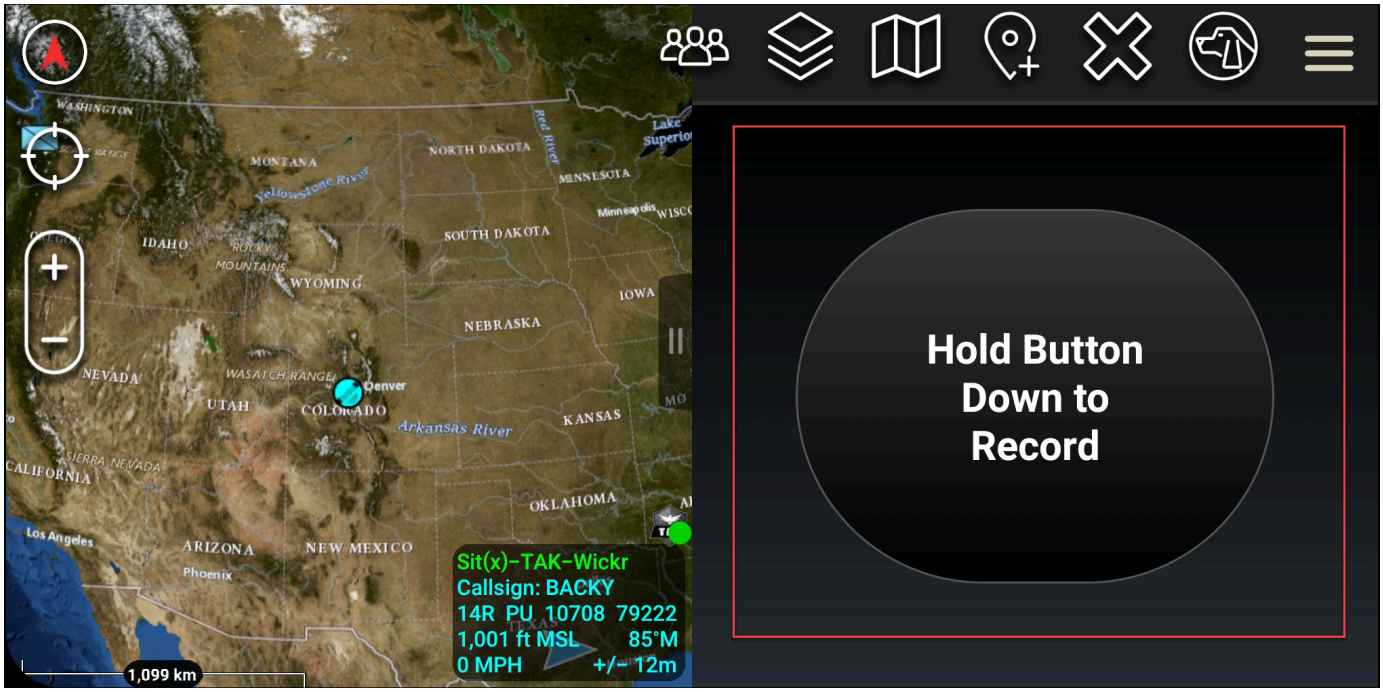
Sie können eine sichere Sprachnachricht (Push-to-talk) im Wickr-Plugin für ATAK senden.

Führen Sie das folgende Verfahren aus, um eine sichere Sprachnachricht zu senden.

1. Öffnen Sie ein Chat-Fenster.
2. Wählen Sie oben auf dem Bildschirm das Push-to-Talk-Symbol aus, das durch ein Symbol einer Person angezeigt wird, die spricht.



3. Wählen und halten Sie die Schaltfläche Halten nach unten zum Aufzeichnen.



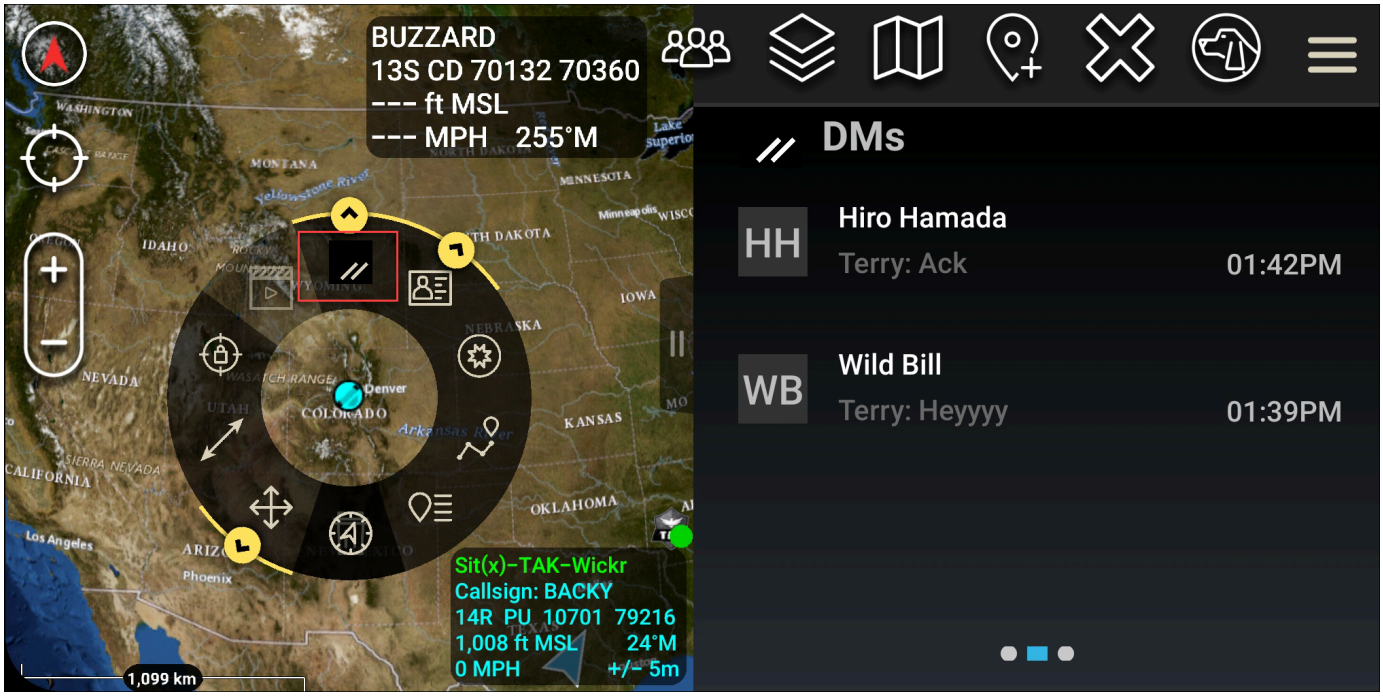
4. Notieren Sie Ihre Nachricht.
5. Nachdem Sie Ihre Nachricht aufgezeichnet haben, lassen Sie die zu sendende Schaltfläche los.

Pinwheel (Quick Access)

Das Pinwheel- oder Quick-Access-Feature wird für one-one-one Gespräche oder direkte Nachrichten verwendet.

Führen Sie das folgende Verfahren aus, um das Pinwheel zu verwenden.

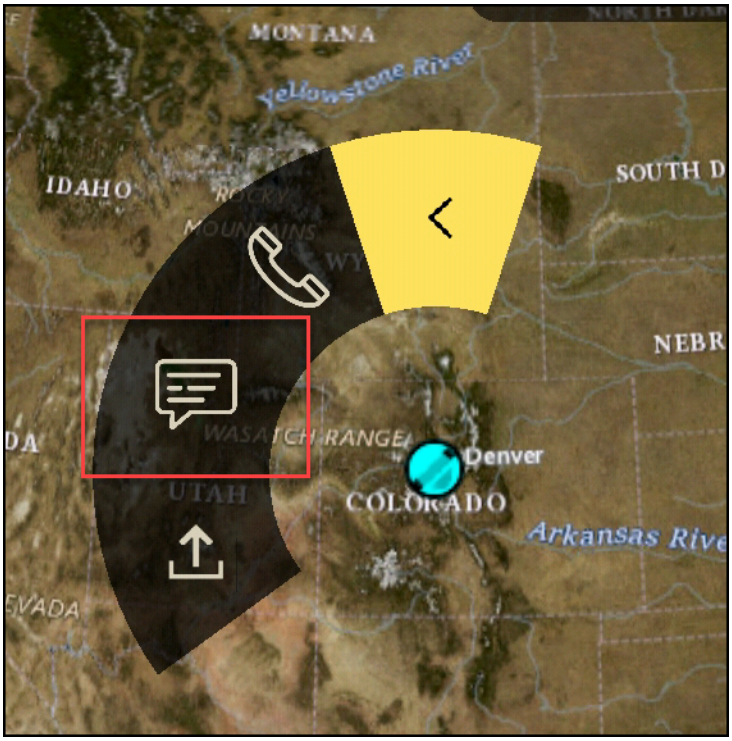
1. Öffnen Sie gleichzeitig die geteilte Bildschirmansicht der ATAK-Map und des Plugins Wickr für ATAK. Die Karte zeigt Ihre Teammitglieder oder Ressourcen in der Kartenansicht an.
2. Wählen Sie das Benutzersymbol, um das Pinwheel zu öffnen.
3. Wählen Sie das Wickr-Symbol, um die verfügbaren Optionen für den ausgewählten Benutzer anzuzeigen.



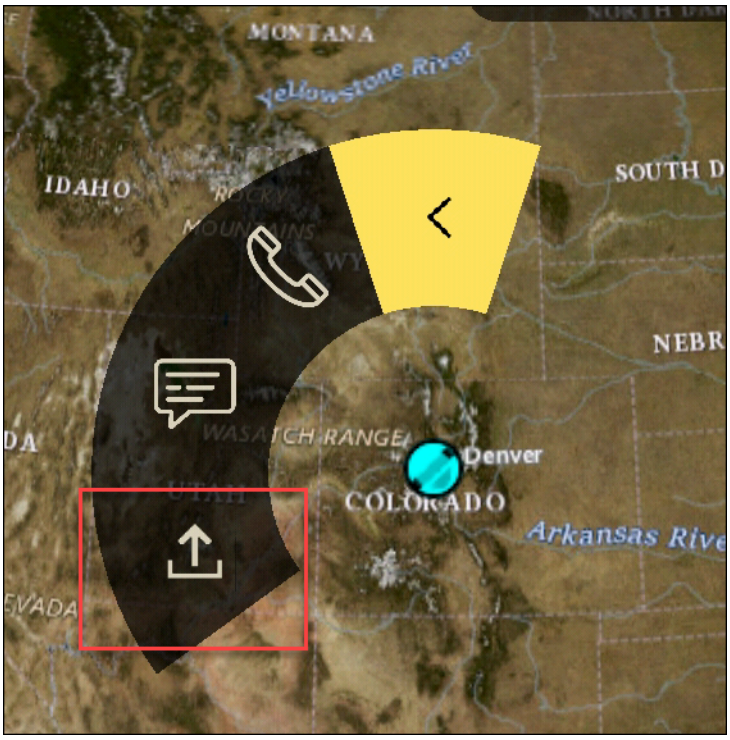
4. Wählen Sie auf dem Pinwheel eines der folgenden Symbole aus:

   - Telefon : Wählen Sie zum Aufrufen aus.

   - Nachricht : Wählen Sie zum Chatten.



- Datei senden: Wählen Sie , um eine Datei zu senden.



Navigation

Die Plugin-Benutzeroberfläche enthält drei Plugin-Ansichten, die durch die blauen und blauen Formen unten rechts auf dem Bildschirm angezeigt werden. Swipe nach links und rechts, um zwischen den Ansichten zu navigieren.

- Ansicht „Kontakte“: Erstellen einer direkten Nachrichtengruppe oder einer Chatroom-Konversation.
- DMs-Ansicht: Erstellen Sie eine one-to-one Konversation. Die Chat-Funktionalität funktioniert wie in der nativen Wickr-App. Mit dieser Funktion können Sie in der Kartenansicht bleiben und mit anderen im Plugin kommunizieren.
- Raumansicht: Die vorhandenen Räume in der nativen App werden portiert. Alles, was im Plugin gemacht wird, spiegelt in der nativen Wickr-App wider.

> **Note**
>
> Bestimmte Funktionen, wie das Löschen eines Raums, können nur in der nativen App und persönlich ausgeführt werden, um unbeabsichtigte Änderungen durch Benutzer und Störungen durch Feldgeräte zu verhindern.

Liste der Ports und Domänen, die zugelassen werden sollen

Um sicherzustellen, dass Wickr korrekt funktioniert, listen Sie die folgenden Ports auf:

Ports

- TCPPort 443 (für Nachrichten und Anlagen)
- UDPPorts 16384-16584 (zum Anrufen)

Domänen und Adressen, die auf die Zulassungsliste gesetzt werden sollen, nach Regionen

Wenn Sie alle möglichen Anrufdomänen und Server-IP-Adressen auf eine Zulassungsliste setzen müssen, finden Sie in der folgenden Liste potenzieller IP-Adressen CIDRs nach Regionen aufgelistet. Überprüfen Sie diese Liste regelmäßig, da sie sich ändern kann.

> **Note**
>
> Registrierungs- und Bestätigungs-E-Mails werden von donotreply@wickr.email gesendet.

USA Ost (Nord-Virginia)

Domänen:	• gw-pro-prod.wickr.com • api.messaging. wickr.us-east-1.amazonaws.com
CIDRAdressen:	• 44.211.195.0/27 • 44,213,83,32/28
IP-Adressen:	• 44.211.195.0 • 44,211,195,1 • 44,211,195,2 • 44,211,159,3 • 44,211,195,4 • 44,211,195,5 • 44,211,159,6 • 44,211,159,7 • 44,211,159,8 • 44,211,195,9 • 44,211,195,10 • 44,211,195,11 • 44,211,195,12 • 44,211,195,13 • 44,211,195,14 • 44,211,195,15 • 44,211,195,16 • 44,211,195,17 • 44,211,195,18

- 44,211,195,19
- 44,211,195,20
- 44,211,195,21
- 44,211,195,22
- 44,211,195,23
- 44,211,195,24
- 44,211,195,25
- 44,211,195,26
- 44,211,195,27
- 44,211,195,28
- 44,211,195,29
- 44,211,195,30
- 44,211,195,31
- 44,213,83,32
- 44,213,83,33
- 44,213,83,34
- 44,213,83,35
- 44,213,83,36
- 44,213,83,37
- 44,213,83,38
- 44,213,83,39
- 44,213,83,40
- 44,213,83,41
- 44,213,83,42
- 44,213,83,43
- 44,213,83,44
- 44,213,83,45
- 44,213,83,46
- 44,213,83,47

Asien-Pazifik (Singapur)

Domäne:	• api.messaging. wickr.ap-southeast-1.amazonaws.com
CIDRAdressen:	• 47.129.23.144/28
IP-Adressen:	• 47.129.23.144 • 47,129,23,145 • 47,129,23,146 • 47,129,23,147 • 47,129,23,148 • 47,129,23,149 • 47,129,23,150 • 47,129,23,151 • 47,129,23,152 • 47,129,23,153 • 47,129,23,154 • 47,129,23,155 • 47,129,23,156 • 47,129,23,157 • 47,129,23,158 • 47,129,23,159

Asien-Pazifik (Sydney)

Domäne:	• api.messaging. wickr.ap-southeast-2.amazonaws.com
CIDRAdressen:	• 3.27.180.208/28
IP-Adressen:	• 3.27.180.208 • 3,27,180,209

	• 3,27,180,210 • 3,27,180,211 • 3,27,180,212 • 3,27,180,213 • 3,27,180,214 • 3,27,180,215 • 3,27,180,216 • 3,27,180,217 • 3,27,180,218 • 3,27,180,219 • 3,27,180,220 • 3,27,180,221 • 3,27,180,222 • 3,27,180,223

Asien-Pazifik (Tokio)

Domäne:	• api.messaging. wickr.ap-northeast-1.amazonaws.com
CIDRAdressen:	• 57.181.142.240/28
IP-Adressen:	• 57.181.142.240 • 57,181,142,241 • 57,181,142,242 • 57,181,142,243 • 57,181,142,244 • 57,181,142,245 • 57,181,142,246 • 57,181,142,247 • 57,181142,248 • 57,181,142,249

	• 57,181142,250 • 57,181142,251 • 57,181142,252 • 57,181,142,253 • 57,181142,254 • 57,181,142,255

Kanada (Zentral)

Domäne:	• api.messaging. wickr.ca-central-1.amazonaws.com
CIDRAdressen:	• 15.156.152.96/28
IP-Adressen:	• 15.156.152.96 • 15,156,152,97 • 15,156,152,98 • 15,156,152,99 • 15,156,152,100 • 15,156,152,1101 • 15,156,152,102 • 15,156,152,103 • 15,156,152,104 • 15,156,152,105 • 15,156,152,106 • 15,156,152,107 • 15,156,152,108 • 15,156,152,109 • 15,156,152,110 • 15,156,152,111

Europa (Frankfurt)

Domäne:	• api.messaging. wickr.eu-central-1.amazonaws.com
CIDRAdressen:	• 3.78.252.32/28
IP-Adressen:	• 3.78.252.32 • 3,78,252,33 • 3,78,252,34 • 3,78,252,35 • 3,78,252,36 • 3,78,252,37 • 3,78,252,38 • 3,78,252,39 • 3,78,252,40 • 3,78,252,41 • 3,78,252,42 • 3,78,252,43 • 3,78,252,44 • 3,78,252,45 • 3,78,252,46 • 3,78,252,47

Europa (London)

Domäne:	• api.messaging. wickr.eu-west-2.amazonaws.com
CIDRAdressen:	• 13.43.91.48/28
IP-Adressen:	• 13.43.91.48 • 13,43,91,49

	• 13,43,91,50 • 13,43,91,51 • 13,43,91,52 • 13,43,91,53 • 13,43,91,54 • 13,43,91,55 • 13,43,91,56 • 13,43,91,57 • 13,43,91,58 • 13,43,91,59 • 13,43,91,60 • 13,43,91,61 • 13,43,91,62 • 13,43,91,63

Europa (Stockholm)

Domäne:	• api.messaging. wickr.eu-north-1.amazonaws.com
CIDRAdressen:	• 13.60.1.64/28
IP-Adressen:	• 13.60.1.64 • 13,601,65 • 13,601,66 • 13,601,67 • 13,60,1,68 • 13,601,69 • 13,601,70 • 13,601,71 • 13,601,72 • 13,601,73

	• 13,601,74 • 13,601,75 • 13,601,76 • 13,601,77 • 13,601,78 • 13,601,79

Europa (Zürich)

Domäne:	• api.messaging. wickr.eu-central-2.amazonaws.com
CIDRAdressen:	• 16.63.106.224/28
IP-Adressen:	• 16.63.106.224 • 16,63,106,225 • 16,63,106,226 • 16,63,106,227 • 16,63,106,228 • 16,63,106,229 • 16,63,106,230 • 16,63,106,231 • 16,63,106,232 • 16,63,106,233 • 16,63,106,234 • 16,63,106,235 • 16,63,106,236 • 16,63,106,237 • 16,63,106,238 • 16,63,106,239

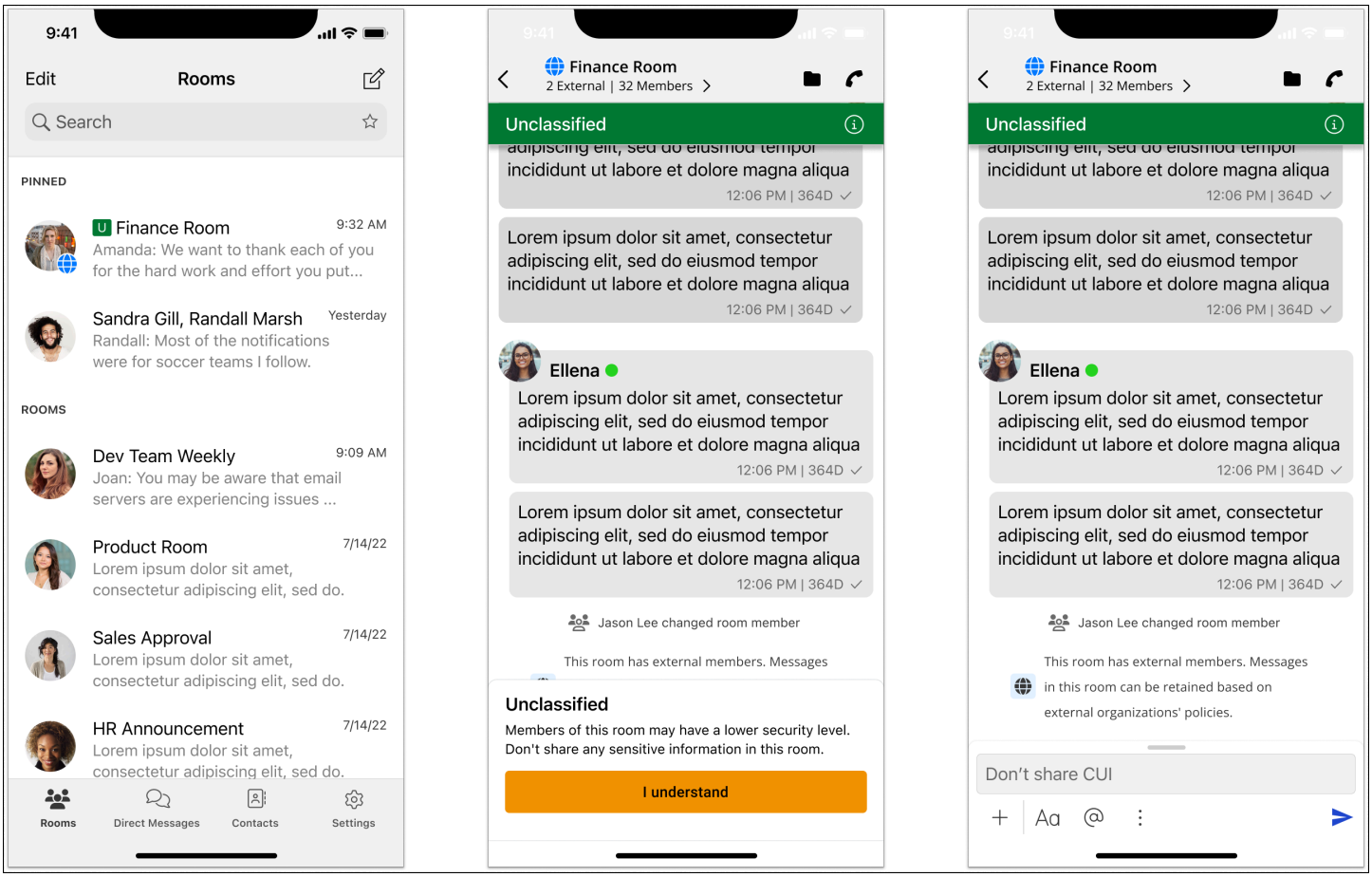
AWS GovCloud (US-West)

Domäne:	• api.messaging.wickr. us-gov-west-1.amazonaws.com
CIDRadressen:	• 3.30.186.208/28
IP-Adressen:	• 3.30.186.208 • 3,30,186,209 • 3,30,186,210 • 3,30,186,211 • 3,30,186,212 • 3,30,186,213 • 3,30,186,214 • 3,30,186,1215 • 3,30,186,216 • 3,30,186,1217 • 3,30,186,218 • 3,30,186,1219 • 3,30,186,220 • 3,30,186,221 • 3,30,186,222 • 3,30,186,223

GovCloud Grenzüberschreitende Klassifikation und Föderation

AWS Wickr bietet einen auf GovCloud Benutzer zugeschnittenen WickrGov Client. Die GovCloud Federation ermöglicht die Kommunikation zwischen GovCloud Benutzern und kommerziellen Benutzern. Die Funktion zur grenzüberschreitenden Klassifizierung ermöglicht es GovCloud Benutzern, Konversationen an der Benutzeroberfläche zu ändern. Als GovCloud Benutzer müssen Sie strenge Richtlinien zur behördlich festgelegten Klassifizierung einhalten. Wenn GovCloud Benutzer Gespräche mit kommerziellen Benutzern (Enterprise, AWS Wickr, Gastbenutzer) führen, werden ihnen die folgenden nicht klassifizierten Warnungen angezeigt:

- Ein U-Tag in der Raumliste
- Eine nicht klassifizierte Bestätigung auf dem Nachrichtenbildschirm
- Ein nicht klassifiziertes Banner über der Konversation



> **Note**
>
> Diese Warnungen werden nur angezeigt, wenn sich ein GovCloud Benutzer mit externen Benutzern unterhält oder Teil eines Raums ist. Sie verschwinden, wenn die externen Benutzer die Konversation verlassen. In Konversationen zwischen GovCloud Benutzern werden keine Warnungen angezeigt.

Benutzer in AWS Wickr verwalten

Im Bereich Benutzer von AWS Management Console for Wickr können Sie aktuelle Wickr-Benutzer und -Bots einsehen und deren Details ändern.

Themen

Team-Verzeichnis

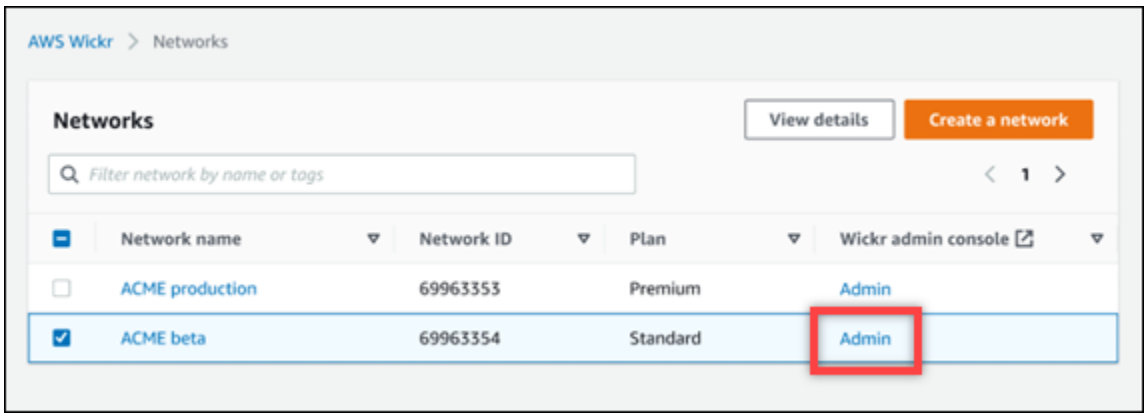
Sie können aktuelle Wickr-Benutzer anzeigen und ihre Details im Benutzerbereich von AWS Management Console for Wickr ändern.

Themen

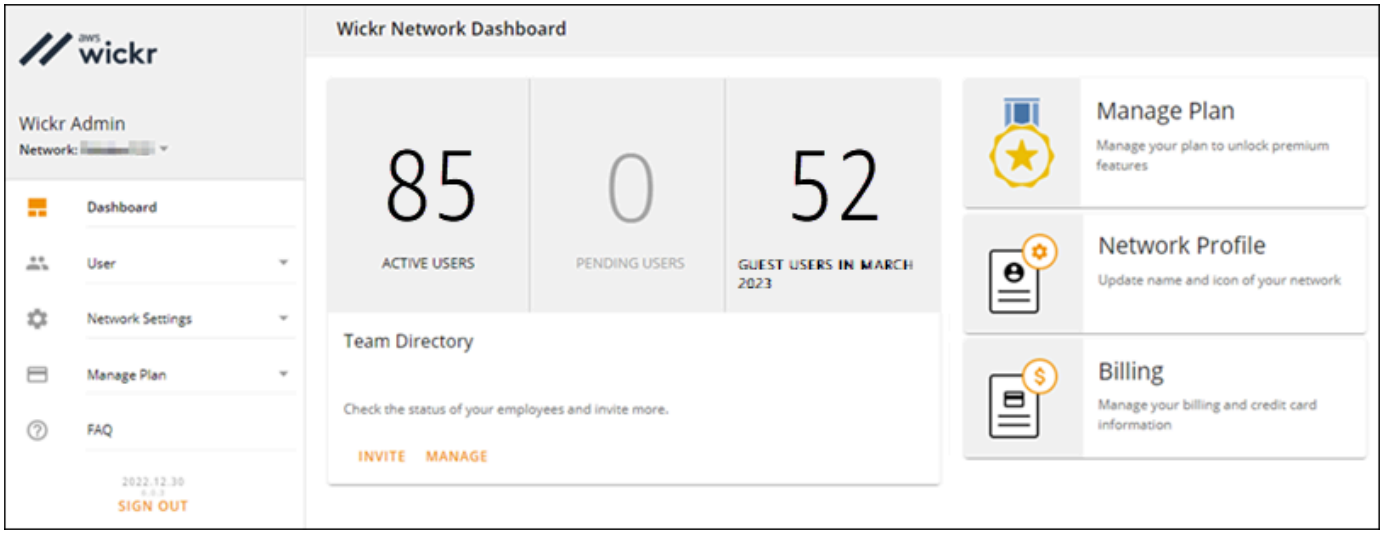
Anzeigen von Benutzern

Gehen Sie wie folgt vor, um Benutzer anzuzeigen, die in Ihrem Wickr-Netzwerk registriert sind.

1. Öffnen Sie das AWS Management Console für Wickr unter https://console.aws.amazon.com/wickr/.
2. Wählen Sie auf der Seite Netzwerke den Link Admin, um zur Wickr Admin Console für dieses Netzwerk zu navigieren.



Sie werden zur Wickr Admin Console für ein bestimmtes Netzwerk weitergeleitet.



3. Wählen Sie im Navigationsbereich der Wickr Admin Console Benutzer und dann Teamverzeichnis aus.

   Auf der Teamverzeichnis-Seite werden Benutzer angezeigt, die in Ihrem Wickr-Netzwerk registriert sind, einschließlich ihres Namens, ihrer E-Mail-Adresse, der zugewiesenen Sicherheitsgruppe und ihres aktuellen Status. Für aktuelle Benutzer können Sie ihre Geräte anzeigen, ihre Daten bearbeiten, sie sperren, löschen und zu einem anderen Wickr-Netzwerk wechseln.

Benutzer erstellen

Gehen Sie wie folgt vor, um einen Benutzer zu erstellen.

1. Öffnen Sie das AWS Management Console für Wickr unter https://console.aws.amazon.com/wickr/.

2. Wählen Sie auf der Seite Netzwerke den Link Admin, um zur Wickr Admin Console für dieses Netzwerk zu navigieren.

   Sie werden zur Wickr Admin Console für ein bestimmtes Netzwerk weitergeleitet.
3. Wählen Sie im Navigationsbereich der Wickr Admin Console Benutzer und dann Teamverzeichnis aus.
4. Wählen Sie Neuen Benutzer erstellen.
5. Geben Sie in dem daraufhin angezeigten Formular den Vor- und Nachnamen, die Landesvorwahl, die Telefonnummer und die E-Mail-Adresse des Benutzers ein. Die E-Mail-Adresse ist das einzige Feld, das erforderlich ist. Achten Sie darauf, die passende Sicherheitsgruppe für den Benutzer auszuwählen. Wickr sendet eine Einladungs-E-Mail an die Adresse, die Sie für den Benutzer angegeben haben.
6. Wählen Sie Erstellen.

   Eine E-Mail wird an den Benutzer gesendet. Die E-Mail enthält Download-Links für die Wickr-Client-Anwendungen und einen Link zur Registrierung für Wickr. Wenn sich Benutzer über den Link in der E-Mail für Wickr registrieren, ändert sich ihr Status im Wickr-Teamverzeichnis von Ausstehend auf Aktiv.

Benutzer bearbeiten

Gehen Sie wie folgt vor, um einen Benutzer zu bearbeiten.

1. Öffnen Sie das AWS Management Console für Wickr unter https://console.aws.amazon.com/wickr/.
2. Wählen Sie auf der Seite Netzwerke den Link Admin, um zur Wickr Admin Console für dieses Netzwerk zu navigieren.

   Sie werden zur Wickr Admin Console für ein bestimmtes Netzwerk weitergeleitet.
3. Wählen Sie im Navigationsbereich der Wickr Admin Console Benutzer und dann Teamverzeichnis aus.
4. Wählen Sie das vertikale Ellipsensymbol neben dem Namen des Benutzers, den Sie löschen möchten.
5. Sie können eine der folgenden Optionen wählen:

- Geräte — Sehen Sie sich die Geräte an, die der Benutzer mit dem Wickr-Client konfiguriert hat.
- Bearbeiten — Bearbeiten Sie die Benutzerdetails wie Name, Landesvorwahl, Telefonnummer (optional) und zugewiesene Sicherheitsgruppe.
- Sperren — Sperren Sie den Benutzer, sodass er sich im Wickr-Client nicht bei Ihrem Wickr-Netzwerk anmelden kann. Wenn Sie einen Benutzer sperren, der derzeit im Client in Ihrem Wickr-Netzwerk angemeldet ist, wird dieser Benutzer automatisch abgemeldet.
- Löschen — Löscht den Benutzer aus Ihrem Wickr-Netzwerk.

Löschen von Benutzern

Gehen Sie wie folgt vor, um einen Benutzer zu löschen.

1. Öffnen Sie das AWS Management Console für Wickr unter https://console.aws.amazon.com/wickr/.
2. Wählen Sie auf der Seite Netzwerke den Link Admin, um zur Wickr Admin Console für dieses Netzwerk zu navigieren.

   Sie werden zur Wickr Admin Console für ein bestimmtes Netzwerk weitergeleitet.
3. Wählen Sie im Navigationsbereich der Wickr Admin Console Benutzer und dann Teamverzeichnis aus.
4. Wählen Sie das vertikale Ellipsensymbol neben dem Namen des Benutzers, den Sie löschen möchten.
5. Wählen Sie Löschen, um den Benutzer zu löschen.

   Wenn Sie einen Benutzer löschen, kann sich dieser Benutzer im Wickr-Client nicht mehr bei Ihrem Wickr-Netzwerk anmelden.

Benutzer auf einmal löschen

Sie können Wickr-Netzwerkbenutzer im Benutzerbereich der Wickr Admin-Konsole für Wickr massenweise löschen und sperren.

> **Note**
>
> Die Option zum Massenlöschen von Benutzern gilt nur, wenn SSO nicht aktiviert ist.

Gehen Sie wie folgt vor, um Ihre Wickr-Netzwerkbenutzer mithilfe einer CSV-Vorlage massenweise zu löschen.

1. Öffnen Sie das AWS Management Console für Wickr unter https://console.aws.amazon.com/wickr/.
2. Wählen Sie im Navigationsbereich der Wickr Admin Console die Option Benutzer und dann Teamverzeichnis aus.

   Auf der Teamverzeichnis-Seite werden Benutzer angezeigt, die in Ihrem Wickr-Netzwerk registriert sind.
3. Wählen Sie auf der Seite Teamverzeichnis die Option Benutzer verwalten aus.
4. Wählen Sie im Popupfenster „Benutzer verwalten“ die Option „Benutzer löschen“.
5. Laden Sie die CSV-Beispielvorlage herunter. Um die Beispielvorlage herunterzuladen, wählen Sie Vorlage herunterladen.
6. Vervollständigen Sie die Vorlage, indem Sie die E-Mail-Adressen der Benutzer hinzufügen, die Sie massenweise aus Ihrem Netzwerk löschen möchten.
7. Laden Sie die fertige CSV-Vorlage hoch. Sie können die Datei per Drag & Drop in das Upload-Feld ziehen oder eine Datei auswählen.
8. Aktivieren Sie das Kontrollkästchen. Ich bestätige, dass das Löschen eines Benutzers nicht rückgängig gemacht werden kann.
9. Wählen Sie Benutzer löschen.

   > **Note**
   >
   > Diese Aktion beginnt sofort mit dem Löschen von Benutzern und kann mehrere Minuten dauern. Gelöschte Benutzer können sich im Wickr-Client nicht mehr bei Ihrem Wickr-Netzwerk anmelden.

Gehen Sie wie folgt vor, um Ihre Wickr-Netzwerkbenutzer massenweise zu löschen, indem Sie eine CSV-Datei Ihres Teamverzeichnisses herunterladen.

1. Öffnen Sie das AWS Management Console für Wickr unter https://console.aws.amazon.com/wickr/.
2. Wählen Sie im Navigationsbereich der Wickr Admin Console die Option Benutzer und dann Teamverzeichnis aus.

   Auf der Teamverzeichnis-Seite werden Benutzer angezeigt, die in Ihrem Wickr-Netzwerk registriert sind.
3. Wählen Sie in der oberen rechten Ecke der Teamverzeichnis-Seite das CSV-Download-Symbol aus.
4. Nachdem Sie die CSV-Vorlage für das Teamverzeichnis heruntergeladen haben, entfernen Sie die Zeilen mit Benutzern, die nicht gelöscht werden müssen.
5. Wählen Sie auf der Seite Teamverzeichnis die Option Benutzer verwalten aus.
6. Wählen Sie im Popupfenster „Benutzer verwalten“ die Option „Benutzer löschen“.
7. Laden Sie die CSV-Vorlage für das Teamverzeichnis hoch. Sie können die Datei per Drag & Drop in das Upload-Feld ziehen oder eine Datei auswählen.
8. Aktivieren Sie das Kontrollkästchen. Ich bestätige, dass das Löschen eines Benutzers nicht rückgängig gemacht werden kann.
9. Wählen Sie Benutzer löschen.

> **Note**
>
> Diese Aktion beginnt sofort mit dem Löschen von Benutzern und kann mehrere Minuten dauern. Gelöschte Benutzer können sich im Wickr-Client nicht mehr bei Ihrem Wickr-Netzwerk anmelden.

Benutzer massenweise sperren

Sie können Wickr-Netzwerkbenutzer im Benutzerbereich der Wickr Admin Console für Wickr massenweise sperren.

> **Note**
>
> Die Option zur Massensperrung von Benutzern gilt nur, wenn SSO nicht aktiviert ist.

Gehen Sie wie folgt vor, um Ihre Wickr-Netzwerkbenutzer massenweise zu sperren.

1. Öffnen Sie das AWS Management Console für Wickr unter https://console.aws.amazon.com/wickr/.
2. Wählen Sie im Navigationsbereich der Wickr Admin Console die Option Benutzer und dann Teamverzeichnis aus.

   Auf der Teamverzeichnis-Seite werden Benutzer angezeigt, die in Ihrem Wickr-Netzwerk registriert sind.
3. Wählen Sie auf der Seite Teamverzeichnis die Option Benutzer verwalten aus.
4. Wählen Sie im Popupfenster „Benutzer verwalten“ die Option „Benutzer sperren“.
5. Laden Sie die CSV-Beispielvorlage herunter. Um die Beispielvorlage herunterzuladen, wählen Sie Vorlage herunterladen.
6. Vervollständigen Sie die Vorlage, indem Sie die E-Mail-Adressen der Benutzer hinzufügen, die Sie massenweise von Ihrem Netzwerk sperren möchten.
7. Laden Sie die fertige CSV-Vorlage hoch. Sie können die Datei per Drag & Drop in das Upload-Feld ziehen oder eine Datei auswählen.
8. Nachdem Sie die CSV-Datei hochgeladen haben, wählen Sie Benutzer sperren.

> **Note**
>
> Diese Aktion beginnt sofort mit dem Sperren von Benutzern und kann mehrere Minuten dauern. Gesperrte Benutzer können sich im Wickr-Client nicht in Ihrem Wickr-Netzwerk anmelden. Wenn Sie einen Benutzer sperren, der derzeit im Client in Ihrem Wickr-Netzwerk angemeldet ist, wird dieser Benutzer automatisch abgemeldet.

Gastnutzer

Die Wickr-Gastbenutzerfunktion ermöglicht es einzelnen Gastbenutzern, sich beim Wickr-Client anzumelden und mit Wickr-Netzwerkbenutzern zusammenzuarbeiten. Wickr-Administratoren können Gastbenutzer für ihre Wickr-Netzwerke auf der Seite Sicherheitsgruppe der Wickr-Administrationskonsole aktivieren oder deaktivieren.

Nachdem die Funktion aktiviert wurde, können Gastbenutzer, die zu Ihrem Wickr-Netzwerk eingeladen wurden, mit Benutzern in Ihrem Wickr-Netzwerk interagieren. Für die

Gastbenutzerfunktion wird eine Gebühr auf Sie AWS-Konto erhoben. Weitere Informationen zu den Preisen für die Gastbenutzerfunktion finden Sie auf der Preisseite von Wickr unter Preis-Add-ons.

Themen

Aktivieren oder deaktivieren Sie Gastbenutzer

Gehen Sie wie folgt vor, um Gastbenutzer für Ihr Wickr-Netzwerk zu aktivieren oder zu deaktivieren.

1. Öffnen Sie das AWS Management Console für Wickr unter https://console.aws.amazon.com/wickr/.
2. Wählen Sie auf der Seite Netzwerke den Link Admin, um zur Wickr Admin Console für dieses Netzwerk zu navigieren.

   Sie werden zur Wickr Admin Console für ein bestimmtes Netzwerk weitergeleitet.
3. Wählen Sie im Navigationsbereich der Wickr Admin Console Netzwerkeinstellungen und dann Sicherheitsgruppe.
4. Wählen Sie Details für eine bestimmte Sicherheitsgruppe.

   > **Note**
   >
   > Sie können Gastbenutzer nur für einzelne Sicherheitsgruppen aktivieren. Um Gastbenutzer für alle Sicherheitsgruppen in Ihrem Wickr-Netzwerk zu aktivieren, müssen Sie die Funktion für jede Sicherheitsgruppe in Ihrem Netzwerk aktivieren.
5. Wählen Sie auf der Seite mit den Sicherheitsgruppendetails die Registerkarte Federation.
6. Es gibt zwei Bereiche, an denen der Schalter zum Zulassen von Gastbenutzern verfügbar sein wird:

   - Lokaler Verband — Wählen Sie für Netzwerke im Osten der USA (Nord-Virginia) neben dem Abschnitt Lokaler Verband der Seite die Option Bearbeiten aus.

- Globaler Verband — Wählen Sie für alle anderen Netzwerke in anderen Regionen neben dem Bereich Globaler Verband der Seite die Option Bearbeiten aus.

7. Wählen Sie Gastbenutzern erlauben, Gastbenutzer für die Sicherheitsgruppe zu aktivieren, oder deaktivieren Sie die Option, um sie zu deaktivieren.
8. Wählen Sie Speichern, um die Änderung zu speichern und sie für die Sicherheitsgruppe wirksam zu machen.

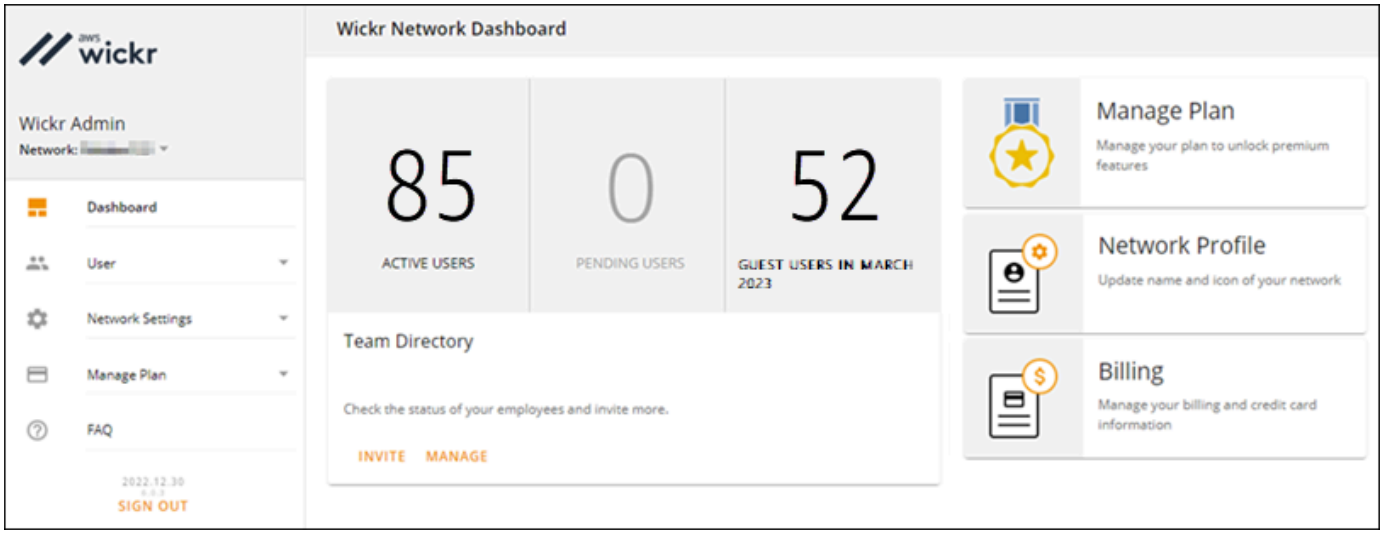
   Registrierte Benutzer in der spezifischen Sicherheitsgruppe in Ihrem Wickr-Netzwerk können jetzt mit Gastbenutzern interagieren. Weitere Informationen finden Sie unter Gastbenutzer im Wickr-Benutzerhandbuch.

Anzahl der Gastbenutzer anzeigen

Gehen Sie wie folgt vor, um die Anzahl der Gastbenutzer für Ihr Wickr-Netzwerk anzuzeigen.

1. Öffnen Sie das AWS Management Console für Wickr unter https://console.aws.amazon.com/wickr/.
2. Wählen Sie auf der Seite Netzwerke den Link Admin, um zur Wickr Admin Console für dieses Netzwerk zu gelangen.

   Sie werden zur Wickr Admin Console für ein bestimmtes Netzwerk weitergeleitet. Auf der Dashboard-Seite wird die Anzahl der Gastbenutzer in Ihrem Wickr-Netzwerk angezeigt, wie im folgenden Beispiel gezeigt.



Monatliche Nutzung anzeigen

Sie können die Anzahl der Gastbenutzer einsehen, mit denen Ihr Netzwerk während eines Abrechnungszeitraums kommuniziert hat. Gehen Sie wie folgt vor, um Ihre monatliche Nutzung einzusehen.

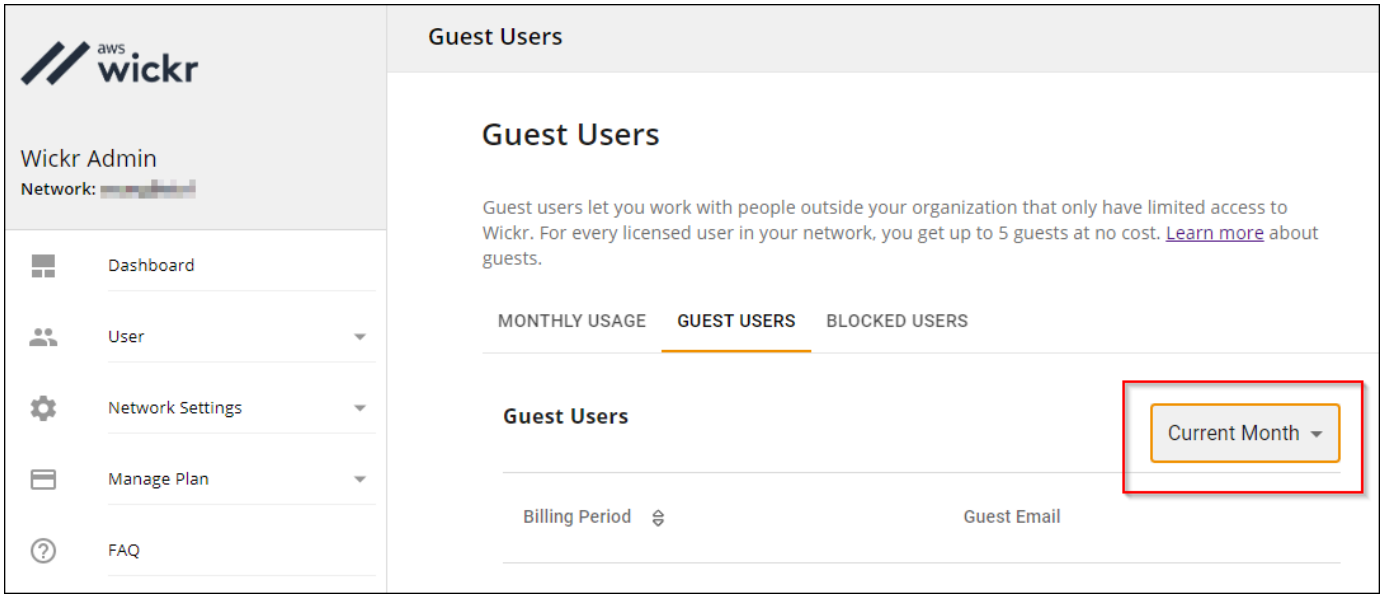
1. Öffnen Sie das AWS Management Console für Wickr unter https://console.aws.amazon.com/wickr/.
2. Wählen Sie auf der Seite Netzwerke den Link Admin, um zur Wickr Admin Console für dieses Netzwerk zu gelangen.
3. Wählen Sie im Navigationsbereich der Wickr Admin Console Benutzer und dann Gastbenutzer aus.
4. Wählen Sie auf der Seite Gastbenutzer den Abschnitt Monatliche Nutzung aus.

> **Note**
>
> Die Rechnungsdaten für Gäste werden alle 24 Stunden aktualisiert.

Gastbenutzer anzeigen

Sie können eine Liste der Gastbenutzer anzeigen, mit denen ein Netzwerkbenutzer während eines bestimmten Abrechnungszeitraums kommuniziert hat. Gehen Sie wie folgt vor, um Ihre Gastbenutzer anzuzeigen.

1. Öffnen Sie das AWS Management Console für Wickr unter https://console.aws.amazon.com/wickr/.
2. Wählen Sie auf der Seite Netzwerke den Link Admin, um zur Wickr Admin Console für dieses Netzwerk zu gelangen.
3. Wählen Sie im Navigationsbereich der Wickr Admin Console Benutzer und dann Gastbenutzer aus.
4. Wählen Sie auf der Seite Gastbenutzer den Abschnitt Gastbenutzer aus.
5. Um Gastbenutzer für einen bestimmten Monat anzuzeigen, wählen Sie den entsprechenden Monat aus dem Drop-down-Menü aus.



Blockieren Sie einen Gastbenutzer

Blockierte Benutzer können mit niemandem in Ihrem Netzwerk kommunizieren.

Um einen Gastbenutzer zu blockieren

1. Öffnen Sie das AWS Management Console für Wickr unter https://console.aws.amazon.com/wickr/.
2. Wählen Sie auf der Seite Netzwerke den Link Admin, um zur Wickr Admin Console für dieses Netzwerk zu gelangen.
3. Wählen Sie im Navigationsbereich der Wickr Admin Console Benutzer und dann Gastbenutzer aus.
4. Wählen Sie auf der Seite Gastbenutzer den Abschnitt Gastbenutzer aus.
5. Im Bereich Gastbenutzer werden die Gastbenutzer angezeigt, die in Ihrem Wickr-Netzwerk kommuniziert haben.
6. Suchen Sie im Bereich Gastbenutzer nach der E-Mail-Adresse des Gastbenutzers, den Sie blockieren möchten.
7. Wählen Sie auf der rechten Seite neben dem Namen des Gastbenutzers die drei Punkte aus und wählen Sie Blockieren aus.
8. Wählen Sie im Popup-Fenster Blockieren aus.
9. Um die Liste der blockierten Benutzer in Ihrem Wickr-Netzwerk anzuzeigen, wählen Sie den Abschnitt Blockierte Benutzer.

Um einen Gastbenutzer zu entsperren

1. Öffnen Sie das AWS Management Console für Wickr unter https://console.aws.amazon.com/wickr/.
2. Wählen Sie auf der Seite Netzwerke den Link Admin, um zur Wickr Admin Console für dieses Netzwerk zu gelangen.
3. Wählen Sie im Navigationsbereich der Wickr Admin Console Benutzer und dann Gastbenutzer aus.
4. Wählen Sie auf der Seite Gastbenutzer den Abschnitt Blockierte Benutzer aus.
5. Im Abschnitt Blockierte Benutzer werden die Gastbenutzer angezeigt, die in Ihrem Wickr-Netzwerk blockiert sind.
6. Suchen Sie im Abschnitt Blockierte Benutzer nach der E-Mail-Adresse des Gastbenutzers, den Sie entsperren möchten.
7. Wählen Sie auf der rechten Seite neben dem Namen des Gastbenutzers die drei Punkte aus und wählen Sie Entsperren aus.
8. Wählen Sie im Popup-Fenster die Option Entsperren aus.

Sicherheit in Wickr AWS

Cloud-Sicherheit bei AWS hat höchste Priorität. Als AWS Als Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung zwischen AWS und du. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud selbst und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die läuft AWS Dienstleistungen in der AWS Cloud. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheit im Rahmen der AWS Compliance-Programme . Weitere Informationen zu den Compliance-Programmen, die für AWS Wickr gelten, finden Sie unter AWS Im Leistungsumfang aufgeschlüsselte Dienstleistungen nach Compliance-Programmen .
- Sicherheit in der Cloud — Ihre Verantwortung wird bestimmt durch AWS Dienst, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung von Wickr anwenden können. Die folgenden Themen zeigen Ihnen, wie Sie Wickr konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie lernen auch, wie Sie andere verwenden AWS Dienste, die Ihnen helfen, Ihre Wickr-Ressourcen zu überwachen und zu sichern.

Themen

Datenschutz in Wickr AWS

Das Tool AWS Modell der gemeinsamen Verantwortung Modell der der gilt für den Datenschutz in AWS Wickr. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre Inhalte zu behalten, die auf dieser Infrastruktur gehostet werden. Sie sind auch verantwortlich für die Sicherheitskonfiguration und die Verwaltungsaufgaben für AWS-Services die Sie verwenden. Weitere Informationen zum Datenschutz finden Sie in der Datenschutzerklärung FAQ. Informationen zum Datenschutz in Europa finden Sie auf der AWS Modell der geteilten Verantwortung und GDPR Blogbeitrag auf der AWS Blog zum Thema Sicherheit.

Aus Datenschutzgründen empfehlen wir Ihnen, AWS-Konto Anmeldeinformationen und richten Sie einzelne Benutzer ein mit AWS IAM Identity Center or AWS Identity and Access Management (IAM). So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Verwenden SieSSL/TLS, um mit zu kommunizieren AWS Ressourcen schätzen. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Einrichtung API und Protokollierung von Benutzeraktivitäten mit AWS CloudTrail. Für Informationen zur Verwendung von CloudTrail Spuren zum Erfassen AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden in der AWS CloudTrail Benutzerleitfaden.
- Verwenden Sie AWS Verschlüsselungslösungen, zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff FIPS 140-3 validierte kryptografische Module benötigen AWS über eine Befehlszeilenschnittstelle oder einenAPI, verwenden Sie einen Endpunkt. FIPS Weitere Informationen zu den verfügbaren FIPS Endpunkten finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Wickr oder anderen zusammenarbeiten AWS-Services mit der Konsole, API AWS CLI, oder AWS SDKs. Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie einem externen Server eine

URL zur Verfügung stellen, empfehlen wir dringend, dass Sie keine Anmeldeinformationen angeben, URL um Ihre Anfrage an diesen Server zu validieren.

Identitäts- und Zugriffsmanagement für AWS Wickr

AWS Identity and Access Management (IAM) ist ein AWS-Service das hilft einem Administrator, den Zugriff auf sicher zu kontrollieren AWS Ressourcen schätzen. IAMAdministratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Wickr-Ressourcen zu verwenden. IAMist ein AWS-Service das Sie ohne zusätzliche Kosten nutzen können.

Themen

Zielgruppe

Wie benutzt du AWS Identity and Access Management (IAM) unterscheidet sich je nach der Arbeit, die Sie in Wickr ausführen.

Dienstbenutzer — Wenn Sie den Wickr-Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen zur Verfügung, die Sie benötigen. Wenn Sie für Ihre Arbeit mehr Wickr-Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Wenn Sie in Wickr nicht auf eine Funktion zugreifen können, finden Sie weitere Informationen unter. Problembehandlung bei AWS Wickr: Identität und Zugriff

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für die Wickr-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf Wickr. Es ist Ihre Aufgabe, zu bestimmen,

auf welche Funktionen und Ressourcen von Wickr Ihre Servicebenutzer zugreifen sollen. Anschließend müssen Sie Anfragen an Ihren IAM Administrator senden, um die Berechtigungen Ihrer Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die grundlegenden Konzepte von zu verstehenIAM. Weitere Informationen darüber, wie Ihr Unternehmen Wickr nutzen IAM kann, finden Sie unterWie arbeitet AWS Wickr mit IAM.

IAMAdministrator — Wenn Sie ein IAM Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff auf Wickr zu verwalten. Beispiele für identitätsbasierte Wickr-Richtlinien, die Sie in verwenden können, finden Sie unter. IAM Beispiele für identitätsbasierte Richtlinien für Wickr AWS

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich anmelden AWS mit Ihren Identitätsdaten. Sie müssen authentifiziert (angemeldet) sein AWS) als Root-Benutzer des AWS-Kontos, als IAM Benutzer oder durch Übernahme einer IAM Rolle.

Sie können sich anmelden bei AWS als föderierte Identität mithilfe von Anmeldeinformationen, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAMIdentity Center) - Nutzer, die Single-Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als föderierte Identität anmelden, hat Ihr Administrator zuvor einen Identitätsverbund mithilfe von Rollen eingerichtet. IAM Wenn Sie darauf zugreifen AWS Wenn Sie den Verbund verwenden, übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich bei der anmelden AWS Management Console oder das AWS Zugangsportal. Weitere Informationen zur Anmeldung bei AWS, siehe So melden Sie sich bei Ihrem an AWS-Konto in der AWS-Anmeldung Benutzerleitfaden.

Wenn Sie darauf zugreifen AWS programmatisch AWS stellt ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, um Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch zu signieren. Wenn Sie es nicht verwenden AWS Tools, Sie müssen Anfragen selbst unterschreiben. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu signieren, finden Sie unter Signieren AWS APIAnfragen im IAMBenutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. Zum Beispiel AWS empfiehlt, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center

Benutzerhandbuch und Verwendung der Multi-Faktor-Authentifizierung () MFA in AWS im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie eine erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle hat AWS-Services und Ressourcen im Konto. Diese Identität wird als AWS-Konto Root-Benutzer. Der Zugriff erfolgt, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie im Benutzerhandbuch unter Aufgaben, für die Root-Benutzeranmeldedaten erforderlich sind. IAM

Verbundidentität

Es hat sich bewährt, menschlichen Benutzern, einschließlich Benutzern, die Administratorzugriff benötigen, vorzuschreiben, für den Zugriff den Verbund mit einem Identitätsanbieter zu verwenden AWS-Services mithilfe temporärer Anmeldeinformationen.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, ein Web-Identitätsanbieter, der AWS Directory Service, das Identity Center-Verzeichnis oder ein beliebiger Benutzer, der zugreift AWS-Services mithilfe von Anmeldeinformationen, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für eine zentralisierte Zugriffsverwaltung empfehlen wir die Verwendung AWS IAM Identity Center. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten und Anwendungen. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? in der AWS IAM Identity Center Benutzerleitfaden.

IAM-Benutzer und -Gruppen

Ein IAMBenutzer ist eine Identität innerhalb Ihres AWS-Konto das über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wir empfehlen, sich nach Möglichkeit auf temporäre Anmeldeinformationen zu verlassen, anstatt IAM Benutzer mit langfristigen Anmeldeinformationen wie Passwörtern und Zugriffsschlüsseln zu erstellen. Wenn Sie jedoch spezielle Anwendungsfälle haben, für die langfristige Anmeldeinformationen von IAM Benutzern

erforderlich sind, empfehlen wir, die Zugriffsschlüssel abwechselnd zu verwenden. Weitere Informationen finden Sie im Benutzerhandbuch unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, für die IAM langfristige Anmeldeinformationen erforderlich sind.

Eine IAMGruppe ist eine Identität, die eine Sammlung von IAM Benutzern spezifiziert. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise eine Gruppe benennen IAMAdminsund dieser Gruppe Berechtigungen zur Verwaltung von IAM Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Wann sollte ein IAM Benutzer (statt einer Rolle) erstellt werden? im IAMBenutzerhandbuch.

IAMRollen

Eine IAMRolle ist eine Identität in deinem AWS-Konto das hat spezifische Berechtigungen. Es ähnelt einem IAM Benutzer, ist jedoch keiner bestimmten Person zugeordnet. Sie können vorübergehend eine IAM Rolle in der übernehmen AWS Management Console indem Sie die Rollen wechseln. Sie können eine Rolle übernehmen, indem Sie einen anrufen AWS CLI or AWS APIOperation oder mithilfe eines benutzerdefiniertenURL. Weitere Informationen zu Methoden zur Verwendung von Rollen finden Sie unter Verwenden von IAM Rollen im IAMBenutzerhandbuch.

IAMRollen mit temporären Anmeldeinformationen sind in den folgenden Situationen nützlich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie im IAMBenutzerhandbuch unter Erstellen einer Rolle für einen externen Identitätsanbieter. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Um zu kontrollieren, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in. IAM Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center Benutzerleitfaden.
- Temporäre IAM Benutzerberechtigungen — Ein IAM Benutzer oder eine Rolle kann eine IAM Rolle übernehmen, um vorübergehend verschiedene Berechtigungen für eine bestimmte Aufgabe zu übernehmen.

- Kontoübergreifender Zugriff — Sie können eine IAM Rolle verwenden, um einer Person (einem vertrauenswürdigen Principal) in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Allerdings mit einigen AWS-Services, Sie können eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zum Unterschied zwischen Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie IAMim Benutzerhandbuch unter Kontoübergreifender Ressourcenzugriff. IAM
- Serviceübergreifender Zugriff — Einige AWS-Services Funktionen in anderen verwenden AWS-Services. Wenn Sie beispielsweise einen Service aufrufen, ist es üblich, dass dieser Service Anwendungen in Amazon ausführt EC2 oder Objekte in Amazon S3 speichert. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Zugriffssitzungen weiterleiten (FAS) — Wenn Sie einen IAM Benutzer oder eine Rolle verwenden, um Aktionen auszuführen in AWS, Sie gelten als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FASverwendet die Rechte des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anfrage AWS-Service um Anfragen an nachgelagerte Dienste zu stellen. FASAnfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, die Interaktionen mit anderen erfordert AWS-Services oder Ressourcen zum Ausfüllen. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS Anfragen finden Sie unter Zugriffssitzungen weiterleiten.
  - Servicerolle — Eine Servicerolle ist eine IAMRolle, die ein Dienst übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM Administrator kann eine Servicerolle von innen heraus erstellen, ändern und löschenIAM. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an ein AWS-Service im IAM-Benutzerhandbuch.
  - Dienstverknüpfte Rolle — Eine dienstverknüpfte Rolle ist eine Art von Servicerolle, die mit einem verknüpft ist AWS-Service. Der Dienst kann die Rolle übernehmen, eine Aktion in Ihrem Namen durchzuführen. Mit Diensten verknüpfte Rollen erscheinen in Ihrem AWS-Konto und gehören dem Dienst. Ein IAM Administrator kann die Berechtigungen für dienstbezogene Rollen anzeigen, aber nicht bearbeiten.
- Anwendungen, die auf Amazon laufen EC2 — Sie können eine IAM Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance ausgeführt werden und AWS CLI or AWS APIAnfragen. Dies ist dem Speichern von Zugriffsschlüsseln innerhalb der EC2 Instanz vorzuziehen. Um eine zuzuweisen AWS Sie erstellen ein EC2 Instanzprofil, das an die Instanz angehängt ist. Sie müssen einer Instanz eine Rolle

zuweisen und sie allen ihren Anwendungen zur Verfügung stellen. Ein Instanzprofil enthält die Rolle und ermöglicht Programmen, die auf der EC2 Instanz ausgeführt werden, temporäre Anmeldeinformationen abzurufen. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Verwenden einer IAM Rolle zur Erteilung von Berechtigungen für Anwendungen, die auf EC2 Amazon-Instances ausgeführt werden.

Informationen darüber, ob Sie IAM Rollen oder IAM Benutzer verwenden sollten, finden Sie im Benutzerhandbuch unter Wann sollte eine IAM Rolle (anstelle eines IAM Benutzers) erstellt werden.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff in AWS indem Sie Richtlinien erstellen und diese anhängen AWS Identitäten oder Ressourcen. Eine Richtlinie ist ein Objekt in AWS das, wenn es einer Identität oder Ressource zugeordnet ist, ihre Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Principal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien sind gespeichert in AWS als JSON Dokumente. Weitere Informationen zur Struktur und zum Inhalt von JSON Richtliniendokumenten finden Sie im IAMBenutzerhandbuch unter Überblick über JSON Richtlinien.

Administratoren können verwenden AWS JSONRichtlinien, um festzulegen, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Um Benutzern die Erlaubnis zu erteilen, Aktionen mit den Ressourcen durchzuführen, die sie benötigen, kann ein IAM Administrator IAM Richtlinien erstellen. Der Administrator kann dann die IAM Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen übernehmen.

IAMRichtlinien definieren Berechtigungen für eine Aktion, unabhängig von der Methode, mit der Sie den Vorgang ausführen. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der abrufen AWS Management Console, der AWS CLI, oder der AWS API.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind Dokumente mit JSON Berechtigungsrichtlinien, die Sie an eine Identität anhängen können, z. B. an einen IAM Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und

unter welchen Bedingungen ausführen können. Informationen zum Erstellen einer identitätsbasierten Richtlinie finden Sie unter IAMRichtlinien erstellen im Benutzerhandbuch. IAM

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem AWS-Konto. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie oder einer Inline-Richtlinie wählen können, finden Sie im IAMBenutzerhandbuch unter Auswahl zwischen verwalteten Richtlinien und Inline-Richtlinien.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM Rollenvertrauensrichtlinien und Amazon S3 S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder AWS-Services.

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können nicht verwenden AWS verwaltete Richtlinien aus IAM einer ressourcenbasierten Richtlinie.

Zugriffskontrolllisten () ACLs

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLsähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON Richtliniendokumentformat.

Amazon S3 S3, AWS WAF, und Amazon VPC sind Beispiele für Dienste, die unterstützenACLs. Weitere Informationen finden Sie unter Übersicht über ACLs die Zugriffskontrollliste (ACL) im Amazon Simple Storage Service Developer Guide.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen — Eine Berechtigungsgrenze ist eine erweiterte Funktion, mit der Sie die maximalen Berechtigungen festlegen, die eine identitätsbasierte Richtlinie einer IAM Entität (IAMBenutzer oder Rolle) gewähren kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die resultierenden Berechtigungen sind eine Schnittmenge der identitätsbasierten Richtlinien der Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen zu Berechtigungsgrenzen finden Sie im IAMBenutzerhandbuch unter Berechtigungsgrenzen für IAM Entitäten.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Sitzungsrichtlinien.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Um zu erfahren, wie AWS bestimmt, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, siehe Bewertungslogik für Richtlinien im IAMBenutzerhandbuch.

AWS verwaltete Richtlinien für AWS Wickr

Es ist einfacher zu verwenden, um Benutzern, Gruppen und Rollen Berechtigungen hinzuzufügen AWS verwaltete Richtlinien, als selbst Richtlinien zu schreiben. Es erfordert Zeit und Fachwissen, um vom IAMKunden verwaltete Richtlinien zu erstellen, die Ihrem Team nur die Berechtigungen gewähren, die es benötigt. Um schnell loszulegen, können Sie unsere verwenden AWS verwaltete Richtlinien. Diese Richtlinien decken allgemeine Anwendungsfälle ab und sind in Ihrem AWS-Konto. Für weitere Informationen über AWS verwaltete Richtlinien finden Sie unter AWS verwaltete Richtlinien im IAMBenutzerhandbuch.

AWS-Services pflegen und aktualisieren AWS verwaltete Richtlinien. Sie können die Berechtigungen nicht ändern in AWS verwaltete Richtlinien. Dienste fügen gelegentlich zusätzliche Berechtigungen zu einem hinzu AWS verwaltete Richtlinie zur Unterstützung neuer Funktionen. Diese Art von Update

betrifft alle Identitäten (Benutzer, Gruppen und Rollen), an welche die Richtlinie angehängt ist. Es ist am wahrscheinlichsten, dass Dienste ein aktualisieren AWS verwaltete Richtlinie, wenn eine neue Funktion eingeführt wird oder wenn neue Operationen verfügbar werden. Dienste entfernen keine Berechtigungen aus einem AWS verwaltete Richtlinie, sodass durch Richtlinienaktualisierungen Ihre bestehenden Berechtigungen nicht beeinträchtigt werden.

AWS verwaltete Richtlinie: AWSWickrFullAccess

Sie können die `AWSWickrFullAccess` Richtlinie an Ihre IAM Identitäten anhängen. Diese Richtlinie gewährt dem Wickr-Dienst volle Administratorrechte, einschließlich der AWS Management Console für Wickr in der AWS Management Console. Weitere Informationen zum Anhängen von Richtlinien an eine Identität finden Sie unter Hinzufügen und Entfernen von IAM Identitätsberechtigungen in der AWS Identity and Access Management Benutzerleitfaden.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `wickr`— Erteilt dem Wickr-Dienst volle Administratorrechte.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "wickr:*",
            "Resource": "*"
        }
    ]
}
```

Wickr aktualisiert auf AWS Verwaltete Richtlinien

Einzelheiten zu Updates anzeigen für AWS verwaltete Richtlinien für Wickr, seit dieser Dienst begonnen hat, diese Änderungen zu verfolgen. Wenn Sie automatische Benachrichtigungen über Änderungen an dieser Seite erhalten möchten, abonnieren Sie den RSS Feed auf der Seite mit dem Verlauf der Wickr-Dokumente.

Änderung	Beschreibung	Datum
AWSWickrFullAccess – Neue Richtlinie.	Wickr hat eine neue Richtlinie hinzugefügt, die dem Wickr-Dienst vollständige Administratorrechte gewährt, einschließlich der Wickr-Administratorkonsole in der AWS Management Console.	28. November 2022
Wickr hat begonnen, Änderungen zu verfolgen	Wickr begann, Änderungen für seine AWS verwaltete Richtlinien.	28. November 2022

Wie arbeitet AWS Wickr mit IAM

Bevor Sie IAM den Zugriff auf Wickr verwalten, sollten Sie sich darüber informieren, welche IAM Funktionen mit Wickr zur Verfügung stehen.

IAMFunktionen, die Sie mit Wickr verwenden können AWS

IAMMerkmal	Wickr-Unterstützung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Nein
Bedingungsschlüssel für die Richtlinie	Nein
ACLs	Nein
ABAC(Tags in Richtlinien)	Nein
Temporäre Anmeldeinformationen	Nein

IAMMerkmal	Wickr-Unterstützung
Hauptberechtigungen	Nein
Servicerollen	Nein
Serviceverknüpfte Rollen	Nein

Um einen Überblick darüber zu erhalten, wie Wickr und andere AWS Dienste funktionieren mit den meisten IAM Funktionen, siehe AWS Dienste, mit denen IAM im IAMBenutzerhandbuch gearbeitet wird.

Identitätsbasierte Richtlinien für Wickr

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identitätsbasierte Richtlinien sind Dokumente mit JSON Berechtigungsrichtlinien, die Sie an eine Identität anhängen können, z. B. an einen Benutzer, eine IAM Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen einer identitätsbasierten Richtlinie finden Sie unter IAMRichtlinien erstellen im Benutzerhandbuch. IAM

Mit IAM identitätsbasierten Richtlinien können Sie zulässige oder verweigerte Aktionen und Ressourcen sowie die Bedingungen angeben, unter denen Aktionen zulässig oder verweigert werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Weitere Informationen zu allen Elementen, die Sie in einer JSON Richtlinie verwenden können, finden Sie in der Referenz zu den IAM JSON Richtlinienelementen im IAMBenutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für Wickr

Beispiele für identitätsbasierte Wickr-Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Wickr AWS

Ressourcenbasierte Richtlinien innerhalb von Wickr

Unterstützt ressourcenbasierte Richtlinien: Nein

Ressourcenbasierte Richtlinien sind JSON Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM Rollenvertrauensrichtlinien und

Amazon S3 S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder AWS-Services.

Um den kontoübergreifenden Zugriff zu ermöglichen, können Sie in einer ressourcenbasierten Richtlinie ein ganzes Konto oder IAM Entitäten in einem anderen Konto als Prinzipal angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource unterscheiden AWS-Konten, muss ein IAM Administrator des vertrauenswürdigen Kontos auch der Prinzipalentität (Benutzer oder Rolle) die Erlaubnis erteilen, auf die Ressource zuzugreifen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie IAMim IAMBenutzerhandbuch unter Kontoübergreifender Ressourcenzugriff.

Politische Maßnahmen für Wickr

Unterstützt Richtlinienaktionen: Ja

Administratoren können verwenden AWS JSONRichtlinien, um festzulegen, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das `Action` Element einer JSON Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie die zugehörigen AWS APIBetrieb. Es gibt einige Ausnahmen, z. B. Aktionen, für die nur Berechtigungen erforderlich sind und für die es keine entsprechende Operation gibt. API Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Eine Liste der Wickr-Aktionen finden Sie unter Von Wickr definierte Aktionen in der AWS Serviceautorisierungsreferenz.

Bei Richtlinienaktionen in Wickr wird vor der Aktion das folgende Präfix verwendet:

```
wickr
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [
      "wickr:action1",
      "wickr:action2"
         ]
```

Beispiele für identitätsbasierte Wickr-Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Wickr AWS

Politische Ressourcen für Wickr

Unterstützt politische Ressourcen: Nein

Administratoren können verwenden AWS JSONRichtlinien, um festzulegen, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das `Resource` JSON Richtlinienelement gibt das Objekt oder die Objekte an, für die die Aktion gilt. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Es hat sich bewährt, eine Ressource mit ihrem Amazon-Ressourcennamen (ARN) anzugeben. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Eine Liste der Wickr-Ressourcentypen und ihrer ARNs Eigenschaften finden Sie unter Von AWS Wickr definierte Ressourcen in der Service Authorization Reference. Informationen darüber, mit welchen Aktionen Sie die ARN einzelnen Ressourcen spezifizieren können, finden Sie unter Von AWS Wickr definierte Aktionen.

Beispiele für identitätsbasierte Wickr-Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Wickr AWS

Bedingungsschlüssel für Richtlinien für Wickr

Unterstützt dienstspezifische Richtlinien-Bedingungsschlüssel: Nein

Administratoren können Folgendes verwenden AWS JSONRichtlinien, um festzulegen, wer Zugriff auf was hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition` Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition` Element angeben, AWS wertet sie mithilfe einer logischen `AND` Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen `OR` Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Sie können einem IAM Benutzer beispielsweise nur dann Zugriff auf eine Ressource gewähren, wenn sie mit seinem IAM Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter IAMRichtlinienelemente: Variablen und Tags.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Um alle zu sehen AWS globale Bedingungsschlüssel finden Sie unter AWS Kontexttasten für globale Bedingungen im IAMBenutzerhandbuch.

Eine Liste der Wickr-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für AWS Wickr in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von AWS Wickr definierte Aktionen.

Beispiele für identitätsbasierte Wickr-Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Wickr AWS

ACLsin Wickr

UnterstütztACLs: Nein

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLsähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON Richtliniendokumentformat.

ABACmit Wickr

Unterstützt ABAC (Tags in Richtlinien): Nein

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen auf der Grundlage von Attributen definiert werden. In AWS, diese Attribute werden Tags genannt. Sie können Tags an IAM Entitäten (Benutzer oder Rollen) und an viele andere anhängen AWS Ressourcen schätzen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt vonABAC. Anschließend entwerfen Sie ABAC Richtlinien, die Operationen zulassen, wenn das Tag des Prinzipals mit dem Tag auf der Ressource übereinstimmt, auf die er zugreifen möchte.

ABACist hilfreich in Umgebungen, die schnell wachsen, und hilft in Situationen, in denen die Richtlinienverwaltung umständlich wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu finden Sie ABAC unter Was ist? ABAC im IAMBenutzerhandbuch. Ein Tutorial mit Schritten zur Einrichtung finden Sie im ABAC Benutzerhandbuch unter Verwenden der attributebasierten Zugriffskontrolle (ABAC). IAM

Temporäre Anmeldeinformationen mit Wickr verwenden

Unterstützt temporäre Anmeldeinformationen: Nein

Etwas AWS-Services funktioniert nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Für zusätzliche Informationen, einschließlich AWS-Services mit temporären Anmeldeinformationen arbeiten, finden Sie unter AWS-Services mit denen IAM im IAMBenutzerhandbuch gearbeitet werden kann.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich bei der anmelden AWS Management Console mit einer beliebigen Methode außer einem Benutzernamen und einem

Passwort. Zum Beispiel, wenn Sie darauf zugreifen AWS Wenn Sie den Single Sign-On-Link (SSO) Ihres Unternehmens verwenden, erstellt dieser Prozess automatisch temporäre Anmeldeinformationen. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Rollenwechsel finden Sie unter Wechseln zu einer Rolle (Konsole) im IAMBenutzerhandbuch.

Sie können temporäre Anmeldeinformationen manuell erstellen, indem Sie AWS CLI or AWS API. Sie können dann diese temporären Anmeldeinformationen für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen unter IAM.

Serviceübergreifende Prinzipalberechtigungen für Wickr

Unterstützt Forward-Access-Sitzungen (FAS): Nein

Wenn Sie einen IAM Benutzer oder eine Rolle verwenden, um Aktionen auszuführen in AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FASverwendet die Rechte des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anfrage AWS-Service um Anfragen an nachgelagerte Dienste zu stellen. FASAnfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, die Interaktionen mit anderen erfordert AWS-Services oder Ressourcen zum Ausfüllen. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für Wickr

Unterstützt Servicerollen: Nein

Eine Servicerolle ist eine IAMRolle, die ein Dienst übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM Administrator kann eine Servicerolle von innen heraus erstellen, ändern und löschenIAM. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an ein AWS-Service im IAM-Benutzerhandbuch.

> **Warning**
>
> Das Ändern der Berechtigungen für eine Servicerolle kann die Wickr-Funktionalität beeinträchtigen. Bearbeiten Sie Servicerollen nur, wenn Wickr Sie dazu anleitet.

Servicebezogene Rollen für Wickr

Unterstützt serviceverknüpfte Rollen: Ja

Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einem verknüpft ist AWS-Service. Der Dienst kann die Rolle übernehmen, eine Aktion in Ihrem Namen durchzuführen. Mit Diensten verknüpfte Rollen erscheinen in Ihrem AWS-Konto und gehören dem Dienst. Ein IAM Administrator kann die Berechtigungen für dienstbezogene Rollen anzeigen, aber nicht bearbeiten.

Einzelheiten zum Erstellen oder Verwalten von dienstbezogenen Rollen finden Sie unter AWS Dienste, die mit IAM funktionieren. Suchen Sie in der Tabelle nach einem Service mit einem `Yes` in der Spalte Service-linked role (Serviceverknüpfte Rolle). Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

Beispiele für identitätsbasierte Richtlinien für Wickr AWS

Standardmäßig hat ein brandneuer IAM Benutzer keine Rechte, irgendetwas zu tun. Ein IAM Administrator muss IAM Richtlinien erstellen und zuweisen, die Benutzern die Erlaubnis geben, den AWS Wickr-Dienst zu verwalten. Dies ist ein Beispiel für eine Berechtigungsrichtlinie.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "wickr:CreateAdminSession",
                "wickr:ListNetworks"
            ],
            "Resource": "*"
        }
    ]
}
```

Diese Beispielrichtlinie gibt Benutzern Berechtigungen zum Erstellen, Anzeigen und Verwalten von Wickr-Netzwerken mithilfe der AWS Management Console für Wickr. Weitere Informationen zu den Elementen einer IAM Grundsatzerklärung finden Sie unterIdentitätsbasierte Richtlinien für Wickr. Informationen zum Erstellen einer IAM Richtlinie anhand dieser JSON Beispieldokumente finden Sie unter Richtlinien erstellen auf der JSON Registerkarte im IAMBenutzerhandbuch.

Themen

- Bewährte Methoden für Richtlinien
- Verwendung der AWS Management Console für Wickr
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand Wickr-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder diese löschen kann. Diese Aktionen können Kosten für Sie verursachen AWS-Konto. Beachten Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Richtlinien und Empfehlungen:

- Fangen Sie an mit AWS verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Um zu beginnen, Ihren Benutzern und Workloads Berechtigungen zu gewähren, verwenden Sie AWS verwaltete Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren. Sie sind in Ihrem verfügbar AWS-Konto. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie Folgendes definieren AWS vom Kunden verwaltete Richtlinien, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS verwaltete Richtlinien oder AWS verwaltete Richtlinien für Jobfunktionen im IAMBenutzerhandbuch.
- Berechtigungen mit den geringsten Rechten anwenden — Wenn Sie Berechtigungen mit IAM Richtlinien festlegen, gewähren Sie nur die Berechtigungen, die für die Ausführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung IAM zum Anwenden von Berechtigungen finden Sie IAMim Benutzerhandbuch unter Richtlinien und Berechtigungen. IAM
- Verwenden Sie Bedingungen in IAM Richtlinien, um den Zugriff weiter einzuschränken — Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen einzuschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um anzugeben, dass alle Anfragen mit gesendet werden müssenSSL. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese über eine bestimmte AWS-Service, wie beispielsweise AWS CloudFormation. Weitere Informationen finden Sie unter IAMJSONRichtlinienelemente: Zustand im IAMBenutzerhandbuch.
- Verwenden Sie IAM Access Analyzer, um Ihre IAM Richtlinien zu validieren, um sichere und funktionale Berechtigungen zu gewährleisten. IAM Access Analyzer validiert neue und bestehende Richtlinien, sodass die Richtlinien der IAM Richtliniensprache (JSON) und den IAM bewährten Methoden entsprechen. IAMAccess Analyzer bietet mehr als 100 Richtlinienprüfungen und

umsetzbare Empfehlungen, um Sie bei der Erstellung sicherer und funktionaler Richtlinien zu unterstützen. Weitere Informationen finden Sie unter IAMAccess Analyzer-Richtlinienvalidierung im IAMBenutzerhandbuch.

- Multi-Faktor-Authentifizierung erforderlich (MFA) — Wenn Sie ein Szenario haben, in dem IAM Benutzer oder ein Root-Benutzer in Ihrem AWS-Konto, schalten Sie MFA für zusätzliche Sicherheit ein. Wenn Sie festlegen möchten, MFA wann API Operationen aufgerufen werden, fügen Sie MFA Bedingungen zu Ihren Richtlinien hinzu. Weitere Informationen finden Sie unter Konfiguration des MFA -geschützten API Zugriffs im IAMBenutzerhandbuch.

Weitere Informationen zu bewährten Methoden finden Sie unter Bewährte Sicherheitsmethoden IAM im IAM Benutzerhandbuch. IAM

Verwendung der AWS Management Console für Wickr

Befestigen Sie das `AWSWickrFullAccess` AWS verwaltete Richtlinie an Ihre IAM Identitäten, um ihnen volle Administratorrechte für den Wickr-Dienst zu gewähren, einschließlich der Wickr-Administratorkonsole in der AWS Management Console. Weitere Informationen finden Sie unterAWS verwaltete Richtlinie: AWSWickrFullAccess.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Dieses Beispiel zeigt, wie Sie eine Richtlinie erstellen könnten, die es IAM Benutzern ermöglicht, die Inline-Richtlinien und verwalteten Richtlinien einzusehen, die mit ihrer Benutzeridentität verknüpft sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe von AWS CLI or AWS API.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
```

```
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Problembehandlung bei AWS Wickr: Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Wickr und auftreten können. IAM

Themen

- Ich bin nicht berechtigt, eine Verwaltungsaktion in der durchzuführen AWS Management Console für Wickr

Ich bin nicht berechtigt, eine Verwaltungsaktion in der durchzuführen AWS Management Console für Wickr

Wenn das Symbol AWS Management Console weil Wickr Ihnen mitteilt, dass Sie nicht berechtigt sind, eine Aktion auszuführen, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Der folgende Beispielfehler tritt auf, wenn der `mateojackson` IAM Benutzer versucht, den AWS Management Console für Wickr, um Wickr-Netzwerke zu erstellen, zu verwalten oder anzuzeigen

in AWS Management Console für Wickr, hat aber nicht die `wickr:CreateAdminSession` Berechtigungen und. `wickr:ListNetworks`

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 wickr:ListNetworks
```

In diesem Fall bittet Mateo seinen Administrator, seine Richtlinien zu aktualisieren, damit er auf die zugreifen kann AWS Management Console für Wickr, der die Aktionen `wickr:CreateAdminSession` und `wickr:ListNetworks` verwendet. Weitere Informationen erhalten Sie unter Beispiele für identitätsbasierte Richtlinien für Wickr AWS und AWS verwaltete Richtlinie: AWSWickrFullAccess.

Compliance-Validierung

Für eine Liste AWS Dienstleistungen im Rahmen bestimmter Compliance-Programme, siehe AWS Dienstleistungen im Geltungsbereich nach Compliance-Programmen . Allgemeine Informationen finden Sie unter AWS Programme zur Einhaltung von Vorschriften .

Sie können Prüfberichte von Drittanbietern herunterladen unter AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen in AWS Artifact.

Ihre Verantwortung für die Einhaltung von Vorschriften bei der Verwendung von Wickr hängt von der Sensibilität Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS bietet die folgenden Ressourcen zur Unterstützung bei der Einhaltung von Vorschriften:

- Schnellstartanleitungen zu Sicherheit und Compliance Schnellstartanleitungen zu — In diesen Bereitstellungshandbüchern werden architektonische Überlegungen erörtert und Schritte für die Bereitstellung sicherheits- und Compliance-orientierter Basisumgebungen beschrieben AWS.
- AWS Ressourcen zur Einhaltung von Vorschriften — Diese Sammlung von Arbeitsmappen und Leitfäden kann auf Ihre Branche und Ihren Standort zutreffen.
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Leitfaden für Entwickler — AWS Config; bewertet, wie gut Ihre Ressourcenkonfigurationen internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Das AWS Der Service bietet einen umfassenden Überblick über Ihren Sicherheitsstatus innerhalb AWS auf diese Weise können Sie überprüfen, ob Sie die Standards und bewährten Verfahren der Sicherheitsbranche einhalten.

Resilienz in AWS Wickr

Das Tool AWS Die globale Infrastruktur basiert auf AWS-Regionen und Availability Zones. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zur AWS-Regionen und Availability Zones, siehe AWS Globale Infrastruktur.

Zusätzlich zu den AWS Wickr ist eine globale Infrastruktur und bietet verschiedene Funktionen zur Unterstützung Ihrer Datenausfallsicherheit und Ihrer Backup-Anforderungen. Weitere Informationen finden Sie unter Datenaufbewahrung.

Sicherheit der Infrastruktur in Wickr AWS

Als verwalteter Dienst ist AWS Wickr geschützt durch AWS Verfahren zur globalen Netzwerksicherheit, die im Whitepaper Amazon Web Services: Sicherheitsprozesse im Überblick beschrieben werden.

Konfiguration und Schwachstellenanalyse in Wickr AWS

Konfiguration und IT-Kontrollen liegen in der gemeinsamen Verantwortung von AWS und Sie, unser Kunde. Weitere Informationen finden Sie auf der AWS Modell der geteilten Verantwortung.

Es liegt in Ihrer Verantwortung, Wickr gemäß den Spezifikationen und Richtlinien zu konfigurieren, Ihre Benutzer regelmäßig anzuweisen, die neueste Version des Wickr-Clients herunterzuladen, sicherzustellen, dass Sie die neueste Version des Wickr-Datenaufbewahrungsbots ausführen, und die Nutzung von Wickr durch Ihre Benutzer zu überwachen.

Bewährte Sicherheitsmethoden für Wickr AWS

Wickr bietet eine Reihe von Sicherheitsfunktionen, die Sie bei der Entwicklung und Implementierung Ihrer eigenen Sicherheitsrichtlinien berücksichtigen sollten. Die folgenden bewährten Methoden sind allgemeine Richtlinien und keine vollständige Sicherheitslösung. Da diese bewährten Methoden

für Ihre Umgebung möglicherweise nicht angemessen oder ausreichend sind, sollten Sie sie als hilfreiche Überlegungen und nicht als bindend ansehen.

Um potenzielle Sicherheitsereignisse im Zusammenhang mit Ihrer Nutzung von Wickr zu verhindern, befolgen Sie diese bewährten Methoden:

- Implementieren Sie den Zugriff mit den geringsten Rechten und erstellen Sie spezielle Rollen, die für Wickr-Aktionen verwendet werden sollen. Verwenden Sie IAM Vorlagen, um eine Rolle zu erstellen. Weitere Informationen finden Sie unter AWS verwaltete Richtlinien für AWS Wickr.
- Greifen Sie auf AWS Management Console für Wickr, indem Sie sich bei der authentifizieren AWS Management Console first. Geben Sie Ihre persönlichen Konsolenanmeldedaten nicht weiter. Jeder Benutzer im Internet kann die Konsole aufrufen, aber er kann sich nur anmelden oder eine Sitzung starten, wenn er über gültige Anmeldeinformationen für die Konsole verfügt.

Überwachung von AWS Wickr

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von AWS Wickr und Ihren anderen AWS Lösungen. AWS bietet die folgenden Überwachungstools, um Wickr zu beobachten, zu melden, wenn etwas nicht stimmt, und gegebenenfalls automatische Maßnahmen zu ergreifen:

- AWS CloudTrailerfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS Kontos getätigt wurden, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Aufrufe erfolgten. Weitere Informationen finden Sie im AWS CloudTrail -Benutzerhandbuch. Weitere Informationen zur Protokollierung von Wickr-API-Aufrufen mithilfe von CloudTrail. Protokollieren von AWS Wickr-API-Aufrufen mit AWS CloudTrail

Protokollieren von AWS Wickr-API-Aufrufen mit AWS CloudTrail

AWS Wickr ist in integriert, einem ServiceAWS CloudTrail, der die Aktionen eines Benutzers, einer Rolle oder eines -AWSServices in Wickr. CloudTrail captures aller API-Aufrufe für Wickr als Ereignisse aufzeichnet. Zu den erfassten Aufrufen gehören Aufrufe von AWS Management Console für Wickr und Code-Aufrufe der Wickr-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3-Bucket aktivieren, einschließlich Ereignissen für Wickr. Wenn Sie keinen Trail konfigurieren, können Sie trotzdem die neuesten Ereignisse in der CloudTrail Konsole unter Ereignisverlauf anzeigen. Anhand der von CloudTrailgesammelten Informationen können Sie die an Wickr gestellte Anfrage, die IP-Adresse, von der die Anfrage gestellt wurde, den Initiator der Anfrage, den Zeitpunkt der Anfrage und zusätzliche Details bestimmen. Weitere Informationen zu CloudTrailfinden Sie im AWS CloudTrail -Benutzerhandbuch.

Wickr-Informationen in CloudTrail

CloudTrail wird beim Erstellen des Kontos AWS-Konto auf Ihrem aktiviert. Wenn eine Aktivität in Wickr auftritt, wird diese Aktivität in einem - CloudTrail Ereignis zusammen mit anderen - AWSServiceereignissen im Ereignisverlauf aufgezeichnet. Sie können in Ihrem AWS-Konto die neusten Ereignisse anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail Ereignisverlauf .

Erstellen Sie für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS-Konto, einschließlich Ereignissen für Wickr, einen Trail. Ein Trail ermöglicht CloudTrail die Bereitstellung von Protokolldateien an einen Amazon S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon-S3-Bucket bereit. Darüber hinaus können Sie andere -AWSServices konfigurieren, um die in den CloudTrail Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- CloudTrail Von unterstützte Services und Integrationen
- Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien aus mehreren Konten

Alle Wickr-Aktionen werden von protokolliert CloudTrail. Aufrufe der `ListNetworks` Aktionen `CreateAdminSession`, und erzeugen beispielsweise Einträge in den CloudTrail Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Anhand der Identitätsinformationen zur Benutzeridentität können Sie Folgendes bestimmen:

- Ob die Anfrage mit Stammbenutzer- oder AWS Identity and Access Management (IAM)-Benutzeranmeldeinformationen ausgeführt wurde.
- Ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer ausgeführt wurde.
- Ob die Anforderung aus einem anderen AWS-Service gesendet wurde

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

Grundlegendes zu Wickr-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, die die Bereitstellung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der

Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordnetes Stacktrace der öffentlichen API-Aufrufe und erscheinen daher nicht in einer bestimmten Reihenfolge.

Das folgende Beispiel zeigt einen - CloudTrail Protokolleintrag, der die `CreateAdminSession` Aktion demonstriert.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-10T07:53:17Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-10T08:19:24Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "CreateAdminSession",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/110.0.0.0 Safari/537.36",
    "requestParameters": {
        "networkId": 56019692
    },
    "responseElements": {
        "sessionCookie": "***",
        "sessionNonce": "***"
    },
```

```
    "requestID": "39ed0e6f-36e9-460d-8a6e-f24be0ec11c5",
    "eventID": "98ccb633-0e6c-4325-8996-35c3043022ac",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

Das folgende Beispiel zeigt einen - CloudTrail Protokolleintrag, der die `CreateNetwork` Aktion demonstriert.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-10T07:53:17Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-10T07:54:09Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "CreateNetwork",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/110.0.0.0 Safari/537.36",
    "requestParameters": {
```

```
        "networkName": "BOT_Network",
        "accessLevel": "3000"
    },
    "responseElements": null,
    "requestID": "b83c0b6e-73ae-45b6-8c85-9910f64d33a1",
    "eventID": "551277bb-87e0-4e66-b2a0-3cc1eff303f3",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

Das folgende Beispiel zeigt einen - CloudTrail Protokolleintrag, der die `ListNetworks` Aktion demonstriert.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-10T12:19:39Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-10T12:29:32Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "ListNetworks",
    "awsRegion": "us-east-1",
```

```
    "sourceIPAddress": "<ip-address>",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/110.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "b9800ba8-541a-43d1-9c8e-efd94d5f2115",
    "eventID": "5fbc83d7-771b-457d-9329-f85163a6a428",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

Das folgende Beispiel zeigt einen - CloudTrail Protokolleintrag, der die `UpdateNetworkdetails` Aktion demonstriert.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-08T22:42:15Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-08T22:42:58Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "UpdateNetworkDetails",
```

```
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36",
    "requestParameters": {
        "networkName": "CloudTrailTest1",
        "networkId": <network-id>
    },
    "responseElements": null,
    "requestID": "abced980-23c7-4de1-b3e3-56aaf0e1fdbb",
    "eventID": "a4dc3391-bdce-487d-b9b0-6f76cedbb198",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

Das folgende Beispiel zeigt einen - CloudTrail Protokolleintrag, der die `TagResource` Aktion demonstriert.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-08T22:42:15Z",
                "mfaAuthenticated": "false"
            }
        }
```

```
    },
    "eventTime": "2023-03-08T23:06:04Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "TagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36",
    "requestParameters": {
        "resource-arn": "<arn>",
        "tags": {
            "some-existing-key-3": "value 1"
        }
    },
    "responseElements": null,
    "requestID": "4ff210e1-f69c-4058-8ac3-633fed546983",
    "eventID": "26147035-8130-4841-b908-4537845fac6a",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

Das folgende Beispiel zeigt einen - CloudTrail Protokolleintrag, der die `ListTagsForResource` Aktion demonstriert.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<access-key-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
```

```
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-08T18:50:37Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-08T18:50:37Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "ListTagsForResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "axios/0.27.2",
    "errorCode": "AccessDenied",
    "requestParameters": {
        "resource-arn": "<arn>"
    },
    "responseElements": {
        "message": "User: <arn> is not authorized to perform: wickr:ListTagsForResource
 on resource: <arn> with an explicit deny"
    },
    "requestID": "c7488490-a987-4ca2-a686-b29d06db89ed",
    "eventID": "5699d5de-3c69-4fe8-b353-8ae62f249187",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```


Analyse-Dashboard

Sie können das Analyse-Dashboard verwenden, um zu sehen, wie Ihr Unternehmen AWS Wickr verwendet. Das folgende Verfahren erklärt, wie Sie mithilfe der AWS Wickr-Konsole auf das Analyse-Dashboard zugreifen.

So greifen Sie auf das Analyse-Dashboard zu

1. Öffnen Sie das AWS Management Console für Wickr unter https://console.aws.amazon.com/wickr/.
2. Wählen Sie im Navigationsbereich Analytics aus.

Auf der Analytics-Seite werden die Metriken für Ihr Netzwerk in verschiedenen Tabs angezeigt.

Auf der Analytics-Seite finden Sie in der oberen rechten Ecke jedes Tabs einen Zeitrahmenfilter. Dieser Filter gilt für die gesamte Seite. Darüber hinaus können Sie in der oberen rechten Ecke jeder Registerkarte die Datenpunkte für den ausgewählten Zeitraum exportieren, indem Sie die verfügbare Exportoption auswählen.

> **Note**
>
> Die gewählte Zeit ist in UTC (Universal Time Coordinated) angegeben.

Die folgenden Tabs sind verfügbar:

- In der Übersicht wird angezeigt:
  - Registriert — Die Gesamtzahl der registrierten Benutzer, einschließlich aktiver und gesperrter Benutzer im Netzwerk in der ausgewählten Zeit. Ausstehende oder eingeladene Benutzer sind nicht enthalten.
  - Ausstehend — Die Gesamtzahl der ausstehenden Benutzer im Netzwerk in der ausgewählten Zeit.
  - Benutzerregistrierung — Das Diagramm zeigt die Gesamtzahl der im ausgewählten Zeitraum registrierten Benutzer.
  - Geräte — Die Anzahl der Geräte, auf denen die App aktiv war.
  - Client-Versionen — Die Anzahl der aktiven Geräte, sortiert nach ihren Client-Versionen.

- Mitglieder zeigt an:
  - Status — Aktive Benutzer im Netzwerk innerhalb des ausgewählten Zeitraums.
  - Aktive Benutzer —
    - Das Diagramm zeigt die Anzahl der aktiven Benutzer im Zeitverlauf an und kann nach Tagen, Wochen oder Monaten (innerhalb des oben ausgewählten Zeitraums) aggregiert werden.
    - Die Anzahl der aktiven Benutzer kann nach Plattform, Client-Version oder Sicherheitsgruppe aufgeschlüsselt werden. Wenn eine Sicherheitsgruppe gelöscht wurde, wird die Gesamtzahl als Gelöscht# angezeigt.

- Meldungen werden angezeigt:
  - Gesendete Nachrichten — Die Anzahl der eindeutigen Nachrichten, die von allen Benutzern und Bots im Netzwerk im ausgewählten Zeitraum gesendet wurden.
  - Anrufe — Anzahl der eindeutigen Anrufe, die von allen Benutzern im Netzwerk getätigt wurden.
  - Dateien — Anzahl der von Benutzern im Netzwerk gesendeten Dateien (einschließlich Sprachnotizen).
  - Geräte — Das Kreisdiagramm zeigt die Anzahl der aktiven Geräte, sortiert nach ihrem Betriebssystem.
  - Client-Versionen — Die Anzahl der aktiven Geräte, sortiert nach ihren Client-Versionen.

Dokumentverlauf

In der folgenden Tabelle werden die Dokumentationsversionen für Wickr beschrieben.

Änderung	Beschreibung	Datum
Grenzüberschreitende Klassifikation und Föderation sind jetzt verfügbar	Die Funktion zur grenzüber schreitenden Klassifiz ierung ermöglicht GovCloud Benutzern Änderungen der Benutzeroberfläche an Konversationen. Weitere Informationen finden Sie unter GovCloud Grenzüber schreitende Klassifizierung und Föderation.	25. Juni 2024
Die Funktion „Lesebest ätigung“ ist jetzt verfügbar	Wickr-Administratoren können jetzt die Lesebestätigungsfu nktion in der Administr atorkonsole aktivieren oder deaktivieren. Weitere Informationen finden Sie unter Lesebestätigungen.	23. April 2024
Global Federation unterstüt zt jetzt den eingeschränkten Verbund und Administratoren können Nutzungsanalysen in der Administratorkonsole einsehen	Global Federation unterstüt zt jetzt den eingeschränkten Verbund. Dies funktioniert für Wickr-Netzwerke in anderen AWS-Regionen. Weitere Informationen finden Sie unter Sicherheitsgruppen. Darüber hinaus können Administr atoren ihre Nutzungsanalysen jetzt im Analytics-Dashboard in der Admin Console einsehen. Weitere Informationen finden	28. März 2024

	Sie unter Analytics-Dashboard.	
Eine dreimonatige kostenlose Testversion des Premium-Plans von AWS Wickr ist jetzt verfügbar	Wickr-Administratoren können jetzt einen dreimonatigen Premium-Testplan für bis zu 30 Benutzer wählen. Während der kostenlosen Testversion sind alle Funktionen des Standard- und Premium-Plans verfügbar, einschließlich unbegrenzter Administratorkontrollen und Datenspeicherung. Die Funktion für Gastbenutzer ist während der kostenlosen Premium-Testversion nicht verfügbar. Weitere Informationen finden Sie unter Abo verwalten.	9. Februar 2024
Die Gastbenutzerfunktion ist allgemein verfügbar und es wurden weitere Administratorsteuerelemente hinzugefügt	Wickr-Administratoren können jetzt auf eine Reihe neuer Funktionen zugreifen, darunter die Liste von Gastbenutzern, die Möglichkeit, Benutzer massenweise zu löschen oder zu sperren, und die Option, Gastbenutzer daran zu hindern, in Ihrem Wickr-Netzwerk zu kommunizieren. Weitere Informationen finden Sie unter Gastbenutzer.	8. November 2023

Wickr ist jetzt in Europa (Frankfurt) erhältlich AWS-Region	Wickr ist jetzt in Europa (Frankfurt) erhältlich. AWS-Region Weitere Informationen finden Sie unter Zugriff auf Wickr.	26. Oktober 2023
Wickr-Netzwerke sind jetzt in der Lage, sich untereinander zu verbünden AWS-Regionen	Wickr-Netzwerke sind jetzt in der Lage, sich untereinander zu verbünden. AWS-Regionen Weitere Informationen finden Sie unter Sicherheitsgruppen.	29. September 2023
Wickr ist jetzt in Europa (London) erhältlich AWS-Region	Wickr ist jetzt in Europa (London) erhältlich. AWS-Region Weitere Informationen finden Sie unter Zugriff auf Wickr.	23. August 2023
Wickr ist jetzt in Kanada (Zentral) verfügbar AWS-Region	Wickr ist jetzt in Kanada (Zentral) erhältlich. AWS-Region Weitere Informationen finden Sie unter Zugreifen auf Wickr.	03. Juli 2023
Die Gastbenutzerfunktion ist jetzt als Vorschau verfügbar	Gastbenutzer können sich beim Wickr-Client anmelden und mit Wickr-Netzwerkbenutzern zusammenarbeiten. Weitere Informationen finden Sie unter Gastbenutzer (Vorschau).	31. Mai 2023

AWSWickr ist jetzt in (US-West) integriert und ist jetzt in AWS GovCloud (US-West) verfügbar als AWS CloudTrail WickrGov	AWSWickr ist jetzt in integriert. AWS CloudTrail Weitere Informationen finden Sie unter AWSAPIWickr-Aufrufe protokollieren mit. AWS CloudTrail Darüber hinaus ist Wickr jetzt in AWS GovCloud (US-West) als verfügbar. WickrGov Weitere Informationen finden Sie AWS WickrGovim AWS GovCloud (US) Benutzerhandbuch.	30. März 2023
Tagging und Erstellung mehrerer Netzwerke	Tagging wird jetzt in AWS Wickr unterstützt. Weitere Informationen finden Sie unter Netzwerk-Tags. In Wickr können jetzt mehrere Netzwerke erstellt werden. Weitere Informationen finden Sie unter Netzwerk erstellen.	7. März 2023
Erstversion	Erste Version des Wickr Administration Guide	28. November 2022

Versionshinweise

Um Ihnen zu helfen, den Überblick über die laufenden Updates und Verbesserungen von Wickr zu behalten, veröffentlichen wir Versionshinweise, in denen die letzten Änderungen beschrieben werden.

Juni 2024

- Die grenzübergreifende Klassifizierung und Föderation ist jetzt für GovCloud Benutzer verfügbar. Weitere Informationen finden Sie unter GovCloud Grenzüberschreitende Klassifizierung und Föderation.

April 2024

- Wickr unterstützt jetzt Lesebestätigungen. Weitere Informationen finden Sie unter Quittungen lesen.

März 2024

- Global Federation unterstützt jetzt den eingeschränkten Verbund, bei dem der globale Verbund nur für ausgewählte Netzwerke aktiviert werden kann, die im Rahmen eines eingeschränkten Verbunds hinzugefügt wurden. Dies funktioniert für Wickr-Netzwerke in anderen AWS-Regionen. Weitere Informationen finden Sie unter Sicherheitsgruppen.
- Administratoren können ihre Nutzungsanalysen jetzt im Analytics-Dashboard in der Admin Console einsehen. Weitere Informationen finden Sie unter Analytics-Dashboard.

Februar 2024

- AWSWickr bietet jetzt eine dreimonatige kostenlose Testversion seines Premium-Plans für bis zu 30 Benutzer an. Zu den Änderungen und Einschränkungen gehören:
  - Alle Funktionen des Standard- und Premium-Tarifs wie unbegrenzte Administratorrechte und Datenspeicherung sind jetzt in der kostenlosen Premium-Testversion verfügbar. Die Funktion für Gastbenutzer ist während der kostenlosen Premium-Testversion nicht verfügbar.

- Die vorherige kostenlose Testversion ist nicht mehr verfügbar. Sie können Ihre bestehende kostenlose Testversion oder Ihren Standardplan auf eine kostenlose Premium-Testversion aktualisieren, falls Sie die kostenlose Premium-Testversion noch nicht genutzt haben. Weitere Informationen finden Sie unter Abo verwalten.

November 2023

- Die Funktion für Gastbenutzer ist jetzt allgemein verfügbar. Zu den Änderungen und Ergänzungen gehören:
  - Möglichkeit, Missbrauch durch andere Wickr-Benutzer zu melden.
  - Administratoren können eine Liste der Gastbenutzer, mit denen ein Netzwerk interagiert hat, sowie die monatliche Nutzungszahl einsehen.
  - Administratoren können Gastbenutzer daran hindern, mit ihrem Netzwerk zu kommunizieren.
  - Zusätzliche Preise für Gastbenutzer.

- Verbesserungen der Admin-Steuerung
  - Möglichkeit zum Massenlöschen/Sperren von Benutzern.
  - Zusätzliche SSO Einstellung zur Konfiguration einer Übergangsfrist für die Tokenaktualisierung.

Oktober 2023

- Verbesserungen
  - Wickr ist jetzt in Europa (Frankfurt) AWS-Region erhältlich.

September 2023

- Verbesserungen
  - Wickr-Netzwerke sind jetzt in der Lage, sich untereinander zu verbünden. AWS-Regionen Weitere Informationen finden Sie unter Sicherheitsgruppen.

August 2023

- Verbesserungen
  - Wickr ist jetzt in Europa (London) AWS-Region erhältlich.

Juli 2023

- Verbesserungen
  - Wickr ist jetzt in Kanada (Zentral) erhältlich. AWS-Region

Mai 2023

- Verbesserungen
  - Unterstützung für Gastbenutzer hinzugefügt. Weitere Informationen finden Sie unter Gastnutzer.

März 2023

- Wickr ist jetzt in integriert AWS CloudTrail. Weitere Informationen finden Sie unter Protokollieren von AWS Wickr-API-Aufrufen mit AWS CloudTrail.
- Wickr ist jetzt in AWS GovCloud (US-West) als verfügbar. WickrGov Weitere Informationen finden Sie AWS WickrGovim AWS GovCloud (US) Benutzerhandbuch.
- Wickr unterstützt jetzt Tagging. Weitere Informationen finden Sie unter Netzwerk-Tags. In Wickr können jetzt mehrere Netzwerke erstellt werden. Weitere Informationen finden Sie unter Schritt 1: Erstellen Sie ein Netzwerk.

Februar 2023

- Wickr unterstützt jetzt das Android Tactical Assault Kit ()ATAK. Weitere Informationen finden Sie unter Aktivieren von ATAK im Wickr Network Dashboard.

Januar 2023

- Single Sign-On (SSO) kann jetzt für alle Tarife konfiguriert werden, einschließlich der kostenlosen Testversion und der Standardversion.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.